MULTI-GIGAHERTZ ENCRYPTED COMMUNICATION USING ELECTRO-OPTICAL CHAOS CRYPTOGRAPHY

A Dissertation
Presented to
The Academic Faculty

By

Nicolas Hugh René Gastaud Gallagher

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
in
Electrical and Computer Engineering

School of Electrical and Computer Engineering
Georgia Institute of Technology
December 2007

MULTI-GIGAHERTZ ENCRYPTED COMMUNICATION USING ELECTRO-OPTICAL CHAOS CRYPTOGRAPHY

Approved by:

Douglas B. Williams, Ph.D., Advisor
Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Nicholas Feamster, Ph.D.
Assistant Professor, School of Computer Science, College of Computing
Georgia Institute of Technology

François J. Malassenet, Ph.D., Advisor
Adjunct Associate Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Faramaz Fekri, Ph.D.
Associate Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Gee-Kung Chang
Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Steven W. McLaughlin, Ph.D.
Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: October 11 2007

to my parents

ACKNOWLEDGMENTS

Reflecting on their Ph.D. years, many have remarked before me that the personal journey is as important, possibly more, then the end research results. I am no different in this respect. Many people made a difference during these years, each imparting valuable lessons. Through this process, I have changed. While I know I cannot possibly remember everybody, I will try nonetheless.

The Ph.D. process is highly shaped by the advisor. I am grateful for the two I had: Profs Williams and Malassenet. They perfected a good cop / bad cop act that always kept me in the right direction and intent on moving forward through the ups and downs that are characteristic of research work. On a more personal level, they took their role as advisors beyond the scientific boundaries. Dr Williams' calm, reassuring support took away much of the stress about that future that other grad students have felt. Dr Malassenet made sure to include us in the many opportunities that were available for "character building" as Calvin's dad would put it that were available around Georgia Tech Lorraine (GTL). It really was not as bad for us as it was for Calvin. Some highlights of these experiences include the Olin College partners' visit, running special problem courses and the GTL Summer Program. There were also many relaxing moments over dinner and *mousse au chocolat*, late night drinks or during ski and sailing trips. Good memories...

A lot of wisdom was imparted during these years. Quite a few times at GTL, I would get "fired up" about some fine point of procedure or protocol. As a result, I heard quite a few times the phrase: "Is this worth getting upset over ?" This would usually stop me dead in my tracks, pondering. Of course, very rarely was it necessary for me to get upset. If there is one thing I am grateful to have learned, I think this is it. Thank you.

I would also like to thank the committee, Drs. Chang, Feamster, Fekri and McLaughlin, for their time and help during the proposal and the defense process. It is always nice to see faculty gracefully take time out of their schedules for these presentations.

Also, both in Metz and in Atlanta, the students have received a lot of help from all the staff. They deserve our recognition and thanks for their hard work and dedication. Many thanks to Jean-Marc, Marc, Sam, Olivier and Muriel (*"notre maman à tous"*) in Metz and Christy, Tammy, Lisa, Catherine in Atlanta. Special thanks to Keith May for all his computer help and not being too strict on the rules of computer use.

And there, we have the basics for a Ph.D. : advisors and lab staff. Fortunately, there have been a lot of friends and activities that liven things up. Each of them contributed in their way to the great experience I had.

I am grateful to the Georgia Tech Ultimate team for getting me out of lab regularly. It was great running from Alabama to North Carolina, from Tennessee to Florida with Scott, Ryan, Graham, Erik, Amrit, Dan and all the others. Thanks guys !

I am also very grateful to the Georgia Tech Sailing Club for providing the escape from the city and fueling my sailing passion. Racing, instructing or just plain sailing was always welcome. Special thanks to the "designated cooking crew" (Emmett, David, Ralph and Konrad) who put in a lot of effort into providing great food at all the New Member BBQs (NMBBQ). I would like to take this opportunity to acknowledge all the time and effort Matthew Widlansky (and his trusted friend Mr Dolphin) puts in to furthering sailing at Georgia Tech. I wish there were many more passionate sailors like him. Sail fast, Matt ! Aaaaarrrrrrrrrrr !

Continuing with the sports club, I would like to thank all my squash partners/opponents for playing some very fun and intense games. A special mention goes to Dr. Chris Paredis for taking the time to help his partners progress. It mad a tremendous difference in my game.

And so, we get to the part on friends and labmates. The Center for Signal and Image Processing at Georgia Tech has many great students: Rajbabu, Maneli, Mina (#1), Toygar, Soner, Amol, Milind, Volkan, Badri, Vince, Jason, Ryan, Marco, Nazanin and Yongseon are just a few of them. Obviously, other labs have great students too : Dario, Tommaso,

Arumugam, Yogesh, Souvik, Andrew, Nitin, Mina (#2), Para, Jeannie, Michael, Benay, Mustapha, Demijan, Mike, Gelsy, Adan, Patricio, Pranav... The list is long. Each one of you is special to me.

This list would not be complete without Will and Martin. I miss my triathlon partners. When do we go back for another Peachtree road race ? With Kevin, we provided many activities for our labmates, from seminars, DCT, food bank volunteering, and picnics to paint ball outings. Grad life would have been different without you !

The original dual Ph.D. crew in Metz made its way to Atlanta, each at his own pace, each bringing his own touch to the fun. Jérôme "Tiptop" Vasseur is best know for his dance floor performances, his great acting skills and his terrific cooking. David "Ninirtz" Boivin is the "Atlanta brunch master" and a former "champion international junior de bowling de Bourgogne". His great jokes (i say this with a straight face), fantastic musical skills and deep knowledge of optical transmission are all very precious to me. Matthieu Bloch, known as Mattlab or "Matthieu ze kid" is a combination of Stakhanov and an ayatollah. Stakhanov because of all the work he gets done and ayatollah because of the yellow and red cards he distributes in seemingly random fashion. Matt, now that I am out, you're next !

I also thank the French Connection, Atlanta chapter for all the great fun that was created. The parties were numerous and intense, and always attracted many different people. I could not ask for better ! Xavier, Julien, Lucie, Ludvic, Max, Stéphanie, Arnaud ("Coach"), Bernard, Laurence, Olivier... So guys, what happened in Atlanta, stays in Atlanta, right ?

I have to add a special line for our "beach volley" team named "Prends ta bâche" for obvious reasons. It felt great to win the Summer 2007 Intramurals Sand Volley Ball tournament with Xavier, Arnaud, Yannick and Vincent. Great games guys !

And then, there is Matthias, my roommate for two years... We recreated a home away from home. Thank you.

I would like to thank my family, my parents and my brother, for their continuing love and support during these years. I am lucky to have them.

TABLE OF CONTENTS

ACKNOWLEDGMENTS iv

LIST OF TABLES x

LIST OF FIGURES xi

SUMMARY xv

CHAPTER 1 INTRODUCTION 1

CHAPTER 2 CHAOS OVERVIEW AND APPLICATION TO TELECOMMUNICATION 4

2.1 Chaos general knowledge 4

2.1.1 Fundamental chaos properties, a first approach 4

2.1.2 Chaos analysis tools 9

2.1.2.1 Phase space 11

2.1.2.2 Spectrum and autocorrelation 13

2.1.2.3 Bifurcation diagram 15

2.2 Chaotic system properties applied to secure communications 17

2.2.1 Chaotic system properties applied to communications 17

2.2.2 Extension to secure communications 21

2.2.3 Cryptography within telecom networks 22

2.3 Experimental optical chaos cryptography 25

2.3.1 All-optical systems 26

2.3.1.1 Injection laser 26

2.3.1.2 External cavity laser 28

2.3.2 Transition towards an opto-electronic dynamic 30

2.3.3 Other opto-electronic chaos cryptography systems 32

2.3.3.1 Wavelength chaos 32

2.3.3.2 Coherence modulation chaos 34

2.3.3.3 Phase chaos 34

2.3.3.4 Intensity chaos 36

2.3.3.5 Comparing results to date 37

2.3.4 OCCULT Contract 38

Conclusion 39

CHAPTER 3 CHAOS GENERATION AND MESSAGE INSERTION 41

3.1 Operating principle 41

3.1.1 Chaos generation 41

3.1.2 Message insertion techniques 45

3.1.2.1 Chaos masking 46

3.1.2.2 Chaos shift keying 47

3.1.2.3 Chaos modulation . . . 49
3.2 Experimental setup . . . 51
3.2.1 Component description . . . 51
3.2.1.1 Laser diode . . . 51
3.2.1.2 Photoreceiver . . . 52
3.2.1.3 Radio frequency amplifier . . . 53
3.2.1.4 Modulator . . . 55
3.2.1.5 Delay line . . . 59
3.2.1.6 Message . . . 61
3.2.1.7 System cost . . . 61
3.2.2 Experimental implementation . . . 62
3.2.2.1 Emitter setup . . . 62
3.2.2.2 Experimental delay measurement . . . 67
3.2.2.3 Bifurcation . . . 68
3.2.2.4 Spectra . . . 72
Conclusion . . . 75

CHAPTER 4 TOWARDS A CRYPTOGRAPHIC SYSTEM . . . 77
4.1 Cryptography notions and context . . . 77
4.1.1 Software approach . . . 79
4.1.1.1 DES . . . 79
4.1.1.2 RSA . . . 81
4.1.1.3 PGP . . . 83
4.1.2 System approach . . . 83
4.1.2.1 Quantum cryptography principle . . . 83
4.1.2.2 Quantum cryptography application . . . 86
4.2 Receiver and system performance . . . 86
4.2.1 Chaotic communication system receiver . . . 86
4.2.2 Synchronization . . . 89
4.2.2.1 Bifurcation parameter β mismatch . . . 95
4.2.2.2 T Delay mismatch . . . 97
4.2.2.3 Phase ϕ mismatch . . . 100
4.2.3 An encrypted communication system . . . 101
4.3 Telecom network encryption integration . . . 110
Conclusion . . . 111

CHAPTER 5 SYSTEM LIMITATIONS AND IMPROVEMENTS . . . 113
5.1 Limitations on system performance . . . 113
5.1.1 Transmission . . . 114
5.1.1.1 Transmission over 50 kilometers . . . 115
5.1.1.2 Transmission over 100 kilometers . . . 117
5.1.2 Synchronization . . . 119
5.1.2.1 Parameter matching . . . 119
5.1.2.2 Component noise . . . 120
5.1.3 Cryptanalysis attacks . . . 121

5.2 Possible improvements . . . 125
5.2.1 Filter . . . 126
5.2.2 Non-linearity . . . 127
5.2.3 Noise suppression . . . 128
5.2.4 Experimental improvement . . . 129
5.2.4.1 Effects of filtering on the chaotic dynamic, route to chaos 129
5.2.4.2 Effects of filtering on the chaotic dynamic, spectral width 130
5.2.4.3 Effects of the filtering on the BER . . . 133
5.2.5 Confidentiality increase possibilities . . . 135
Conclusion . . . 137

CHAPTER 6 BEYOND THE NRZ FORMAT . . . 138
6.1 Advanced optical modulation formats . . . 139
6.1.1 Overview . . . 139
6.1.2 Modulation format choice . . . 140
6.1.3 Message generation methods . . . 141
6.1.3.1 Physically . . . 142
6.1.3.2 In simulation . . . 143
6.2 Simulation aspects . . . 145
6.2.1 Runge-Kutta method . . . 146
6.2.2 Back-to-back communication . . . 147
6.2.3 Transmission . . . 154
6.2.3.1 Fiber propagation effects . . . 154
6.2.3.2 Simulation method . . . 157
6.2.3.3 Simulated transmission . . . 159
Conclusion . . . 163

CONCLUSION . . . 164

REFERENCES . . . 166

LIST OF TABLES

Table 1 Comparative table for different chaotic variables. 37

Table 2 Summary of system component costs 62

Table 3 SMF transmission modules characteristics. 114

Table 4 DCF transmission module characteristics. 116

Table 5 Appropriate settings for different data modulation formats. 144

Table 6 Runge-Kutta a_{rj} coefficients. 147

Table 7 Runge-Kutta b_r coefficients. 147

Table 8 Runge-Kutta c_r coefficients. 147

Table 9 The Bera-Jarque test results. 149

Table 10 The Lilliefors test results. 149

LIST OF FIGURES

Figure 1 Harmonic pendulum principle diagram. 5

Figure 2 Discrete time traces of the logistic map application for different values of the control parameter a. 8

Figure 3 Chua's circuit and non-linearity. 10

Figure 4 Chua's Circuit in periodic regime with $L = 22$ mH. 11

Figure 5 Chua's circuit in a two period periodic regime with $L = 28$ mH. 12

Figure 6 Chua's and Lorenz's attractors. 13

Figure 7 Magnitude sprectra of Chua's circuit in periodic and chaotic regimes. . . 14

Figure 8 Autocorrelation of Chua's circuit in periodic and chaotic regimes. 15

Figure 9 Bifurcation diagram of the logistic map. 17

Figure 10 Chua receiver decomposed into sub-systems. 20

Figure 11 Seven layer OSI model. 22

Figure 12 Schematic diagram of a point-to-point WDM link. 23

Figure 13 Message transmission through an MPLS network. 25

Figure 14 Coupling by injection in between two laser sources. 26

Figure 15 Semiconductor laser coupled to an external cavity of length T_1. 28

Figure 16 Semiconductor laser coupled to an external fiber cavity. 30

Figure 17 Experimental setup of the opto-electronic system. 31

Figure 18 Experimental setup of the wavelength chaos generator. 33

Figure 19 Experimental setup of coherence modulation chaos. 35

Figure 20 Experimental phase chaos generation setup. 36

Figure 21 Experimental intensity chaos generation setup. 36

Figure 22 Experimental Ikeda setup. 42

Figure 23 Principal diagram of the implemented chaos generator. 45

Figure 24 Chaos masking. 47

Figure 25 Non-coherent CSK: principle. 48
Figure 26 Coherent CSK: principle. 49
Figure 27 Chaos modulation: principle. 50
Figure 28 Structure of a DFB laser diode. 52
Figure 29 Typical opto-electronic gain of Miteq photoreceivers. 53
Figure 30 SHF RF amplifier transmission coefficients. 54
Figure 31 Functional diagram of a Mach-Zehnder modulator. 56
Figure 32 Modulation in a Mach-Zehnder interferometer. 57
Figure 33 Electro-optic modulator transmission as a function of frequency. 58
Figure 34 Normalized open-loop electro-optic transfer function. 59
Figure 35 Electro-optic transmission as a function of frequency. 60
Figure 36 Experimental emitter schematic diagram. 64
Figure 37 Picture of the opto-electronic emitter setup. 66
Figure 38 Experimental measurement of the emitter delay. 68
Figure 39 2D experimental bifurcation diagram. 69
Figure 40 Time traces for different optical powers. 71
Figure 41 3D Experimental bifurcation diagram. 72
Figure 42 Electrical experimental chaos spectrum. 73
Figure 43 Optical transmission spectrum for various laser diode output powers (P_1). 74
Figure 44 DES principle diagram. 80
Figure 45 QKD operations diagram. 84
Figure 46 Receiver experimental diagram. 88
Figure 47 Synchronization evaluation experimental setup. 91
Figure 48 Typical example of synchronized time traces, $Y = X$. 92
Figure 49 Inverse synchronization, $Y = -X$. 93
Figure 50 Experimental synchronization observation diagram. 94

Figure 51 Synchronization error as a function of the β parameter computed analytically and numerically, then measured experimentally. 96

Figure 52 Synchronization error as a function of delay mismatch ΔT computed analytically, numerically, and measured experimentally. 99

Figure 53 Synchronization error as a function of the phase ϕ parameter computed analytically, numerically, and measured experimentally. 101

Figure 54 Experimental diagram of BER measurement. 103

Figure 55 Comparative plot of the BER with a 3 GHz message for Bob and Eve as a function of the masking factor α. 105

Figure 56 Bob's eye diagram. 107

Figure 57 Eve's eye diagram. 108

Figure 58 Observed spectra of Alice and Eve for a PRBS7 message at 3 Gbit/s. . . 109

Figure 59 Observed spectra of Alice and Bob for a PRBS7 message at 3 Gbit/s. . . 109

Figure 60 Optical switch for MPλS protocol. 111

Figure 61 Transmission module. 115

Figure 62 Transmission schematic diagram. 115

Figure 63 Encrypted signal eye diagram, $\alpha = 1, 3$. 116

Figure 64 Eye diagram after 50 km transmission and dispersion compensation (BER $= 2 \cdot 10^{-5}$). 117

Figure 65 Eye diagram after 100 km transmission and dispersion compensation (BER $= 5 \cdot 10^{-4}$). 118

Figure 66 Eye diagram after 100 km transmission and dispersion compensation (BER $= 8 \cdot 10^{-6}$). 119

Figure 67 Average mutual information extracted from an experimentally transmitted signal. 125

Figure 68 Experimental emitter diagram with filter. 126

Figure 69 Experimental receiver diagram with filter. 127

Figure 70 Frequency response of two low-pass filters. 128

Figure 71 Bifurcation diagram without filter and modulator bias voltage $V_{B1} = 2.85$ V. 131

Figure 72 Bifurcation diagram with low-pass filter (f_c = 2.7GHz) and modulator bias voltage V_{B1} = 2.85 V. 131

Figure 73 Bifurcation diagram without filter and modulator bias voltage V_{B1} = 0.7 V. 132

Figure 74 Bifurcation diagram with low-pass filter (f_c = 2.7GHz) and modulator bias voltage V_{B1} = 0.7 V. 132

Figure 75 Experimental spectrum of the chaotic dynamics generated by the emitter with a low-pass filter (filter #127) in the feedback loop. P_1 = 6 mW, V_{B1} = 2.85 V, T =42.15 ns. 133

Figure 76 Evolution of the BER with and without RF filter at 2.7 GHz. 134

Figure 77 Intensity chaos system diagram with two delays and two non linearities in the feedback loop. 136

Figure 78 Return-to-zero generation. 143

Figure 79 Carrier suppressed return-to-zero generation. 144

Figure 80 Simulated messages for the different data modulation formats. 145

Figure 81 Typical message probability distribution as a function of recorded amplitude. 150

Figure 82 BER plots. 151

Figure 83 BER plot as a function of message RMS value. 152

Figure 84 BER as a function of noise standard deviation for fixed message amplitudes 1 (dashed) and 0.85 (solid). 153

Figure 85 Propagating chaotic signal. 160

Figure 86 BER evolution as a function of message amplitude after 50 km propagation. 162

Figure 87 BER evolution as a function of message amplitude after 100 km propagation. 162

SUMMARY

Chaotic dynamics are at the center of multiple studies to perfect encrypted communication systems. Indeed, the particular time evolution nature of chaotic signals constitutes the fundamentals of their application to secure telecommunications. The pseudo random signal constitutes the carrier wave for the communication. The information coded on the carrier wave can be extracted with knowledge of the system dynamic evolution law.

This evolution law consists of a second-order delay differential equation in which intervene the various parameters of the physical system setup. The set of precise parameter values forms the key, in a cryptographic sense, of the encrypted transmission.

This thesis work presents the implementation of an experimental encryption system using chaos. The optical intensity of the emitter fluctuates chaotically and serves as carrier wave. A message of small amplitude, hidden inside the fluctuations of the carrier wave, is extracted from the transmitted signal by a properly tuned receiver.

The influence of the message modulation format on the communication quality both in the back to back case and after propagation is investigated numerically.

CHAPTER 1

INTRODUCTION

The security of communications has historically played a determining role in the course of history. Caesar created his own cypher to communicate with his troops [1, 83]. Mary, Queen of Scots, lost her head because her personal cypher was broken. While in jail, she plotted the demise of her political rival, and cousin, Elizabeth, queen of England. With Queen Mary's cypher broken, Elizabeth was able to prove the treachery of her cousin. As a result, a public trial ensued with the sentence being death by decapitation [86]. More recently, during World War II, the Japanese mounted a diversion to trap the remainder of the U.S. Pacific fleet at Midway. The plan included various diversionary attacks to spread out U.S. forces and divert them from the final objective. The effects of these elaborate steps were negated because of the work of the Combat Intelligence Office led by Commander Rochefort. They managed to break the Imperial Japanese Navy's code, JN-25, and therefore, uncover the Japanese battle plan. This advantage was a key factor in the United States' victory at Midway and turned the tides of battle in the Pacific.

These are just a few examples of the potential effects of communication security (or lack thereof). Obviously, the scope and consequences of the proposed research are not expected to be as dramatic as in the examples just cited. Communication security impacts our daily lives in many ways: bank transfers, e-commerce, email privacy, cell phone communications, and many more.

As we have seen, communicating securely is not a new problem. Yet, secure communication is becoming a more and more widespread concern because of the increase in Internet traffic. The traffic volume on the U.S. backbone alone increased from 1 Tbit/month in 1990 to 35000 Tbit/month 10 years later in 2000 [49]. While all of this traffic does not need to be secure, an increasingly high percentage requires some form of security. Computers with traditional software encryption had been unable to keep up with the exploding speed

increase of optical networks. Therefore, novel ways of encryption have been researched.

The proposed research aims to extend a novel form of communication security to modern technology: (multi giga Hertz) optical communication. To do so, we are adding encryption at the physical layer (layer 1) of the open system interconnection (OSI) stack [70]. The aim is not to replace any encryption present at the application layer (layer 7) but to complement it. At the physical layer, the encryption is not performed via algorithms implemented in software, but via a novel form of hardware encryption called *chaos cryptography*.

Chapter 2 relates the discoveries that have led to the emergence and evolution of the field of chaos cryptography: first, the discovery of chaotic phenomena and their fundamental properties and, second, an initial physical implementation (Chua's circuit, Section 2.1). An overview of the research in this field is presented underlining the different research avenues that have been pursued and how our proposed research is positioned within the field. We also look at more recent developments that make use of the power of optics in Section 2.3.

The communication system we propose is divided into two separate entities: the emitter and the receiver. Chapter 3 focuses on the design and properties of the emitter. An architecture is presented, as well as the components required. Emitter performance results are presented. These include bifurcation diagrams and spectral measurements, both in the optical domain and in the radio-frequency (RF) domain.

The communication system receiver is detailed in Chapter 4. The receiver's *raison d'être* is to extract the information transmitted by the emitter (Section 4.2.1). To this purpose, we evaluate the synchronization quality (Section 4.2.2) before determining the communication link quality as measured by the bit error ratio (BER) in Section 4.2.3.

Chapter 5 examines the system limitations in terms of transmission distance (Section 5.1.1), residual parameter mismatch (Section 5.1.2) and security (Section 5.1.3). Improvements are proposed (Section 5.2) to overcome the limitations set forward previously. These consist of appropriate filtering (Section 5.2.1) which improves parameter matching

and reduces noise. The improvement is observed experimentally (Section 5.2.4). A modification to the system architecture is also proposed to counter known cryptography attacks (Section 5.2.5).

Chapter 6 investigates the system from the perspective of the message. Throughout the first 5 chapters of the dissertation, the message is of a fixed non-return-to-zero (NRZ) format. Chapter 6 simulates system behavior and performance with different message modulation formats both in the back-to-back and after transmission.

We then summarize our results and present some avenues for future work in the conclusion.

CHAPTER 2

CHAOS OVERVIEW AND APPLICATION TO TELECOMMUNICATION

We start by explaining the notion of chaotic dynamics. This first approach will lead to a better grasp of the subject matter while introducing some of the analysis tools pertinent to chaotic dynamics, both in the time and spectral domains. Then, we will detail the properties of chaotic dynamics that are applicable to telecommunication (Section 2.2): synchronization capacity between distant chaotic emitter and receiver, pseudo-randomness permitting masking, and compatibility of chaos cryptography with modern optical communication networks. Our system is based on these properties. We will conclude this chapter with a survey of experimental chaos cryptography experimental approaches. This last section will help position the system that we propose with reference to the field.

2.1 Chaos general knowledge

Far from attempting to give a mathematical definition of chaotic behavior, we turn to describing the qualitative characteristics in order to comprehend the properties essential to an application to chaos cryptography. In spite of the presence of chaotic behavior in numerous fields (chemistry, medicine, economics, physics), giving a precise and rigorous definition of chaos starting from experimental observations is very difficult. We will therefore limit ourselves to clarifying the notion of chaotic behavior before defining analysis tools relevant to the characterization of chaotic dynamics.

2.1.1 Fundamental chaos properties, a first approach

Chaos is a behavior observed in certain non-linear dynamical systems. The term "chaos" and the adjective "chaotic" apply to the time evolution of one (or multiple) variables, to a spatial evolution (such as Couette flows in fluid dynamics) or both at the same time (e.g. convection in a Rayleigh-Benard experiment). To simplify, we will limit ourselves to

dynamics subject to a time evolution. A dynamical system can then be described by a state vector $\vec{X}(t)$ whose time evolution can be described by a differential equation of the type:

$$\frac{d}{dt}\vec{X}(t) = \mathcal{F}\left(\vec{X}(t)\right), \tag{1}$$

or in the case of a discrete time application:

$$\vec{X_n} = \mathcal{F}\left(\vec{X}_{n-1}\right). \tag{2}$$

We distinguish two types of dynamical systems: continuous time and discrete time. Two simple examples illustrating these system classes are the oscillating pendulum and the logistic map application. Let us now detail the dynamic behavior of both of them.

The harmonic pendulum comprises a mass *m* fixed to the end of a rod of length *l*. This mass is subject to the gravity field of acceleration *g* and oscillates in the vertical plane (Figure 1).

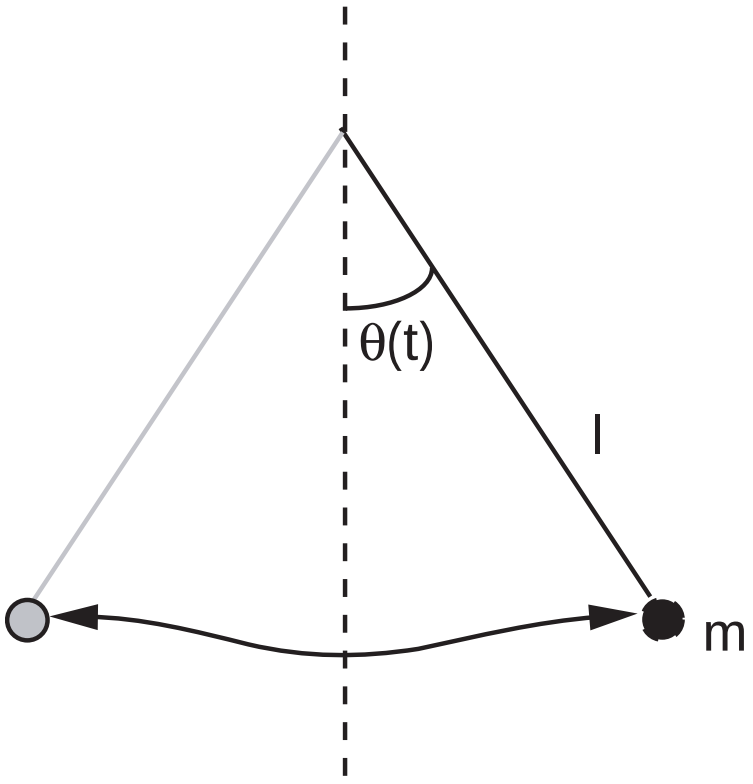


Figure 1: Harmonic pendulum principle diagram.

The variable that describes the oscillations of the pendulum is the angle $\theta(t)$ in between the rod and the vertical axis. There exist two equilibrium positions both on the vertical axis: one below and one above the center of rotation. The first equilibrium position is stable. After a perturbation, the friction force dampens the oscillations and the pendulum returns to its equilibrium position. The second equilibrium position is unstable: the pendulum does not return to its equilibrium position after a perturbation. This behavior is a first example of a dynamical regime for the pendulum.

When the pendulum is released from a position slightly removed from the vertical, another oscillation pattern is followed. The physical laws of motion enable us to write these equations, describing the pendulum motion in the absence of friction forces:

$$F = ml\frac{d^2\theta}{dt^2} = -mg\ \sin\theta \tag{3}$$

$$\frac{d^2\theta}{dt^2} + \frac{g}{l}\ \sin\theta = 0 \tag{4}$$

For oscillations of small amplitudes, the linear approximation $\sin\theta \approx \theta$ helps solve the now linear equation (4). The solution is a simple periodic motion:

$$\theta = \theta_0 \cos(\omega t + \phi) \tag{5}$$

$$\omega = \sqrt{\frac{g}{l}} = \frac{2\pi}{T} \tag{6}$$

where ω is the angular frequency of the pendulum, T the period, and ϕ the initial angular phase at time $t = 0$.

However, when the movement amplitude increases, the linear approximation $\sin\theta \approx \theta$ is no longer valid. The solution to the differential equation changes as the system is now non-linear and harmonic frequencies that are integer multiples of the fundamental frequency now appear. With this harmonic pendulum, a single system can exhibit different dynamical behaviors (equilibrium (stable or unstable), periodic motion at one fundamental frequency or with various frequencies integer multiples of the fundamental).

As an example of a discrete time dynamical system, we choose as the logistic map

defined by:

$$x_{n+1} = a \cdot x_n(1 - x_n), \tag{7}$$

where n varies from 0 to N and a represents the weight of a non-linear transformation (i.e. a second order polynomial: $x(1 - x)$) in the iterative process: $x_{n+1} = F_{NL}(x_n)$. Depending on the value of a, the logistic map application will exhibit different steady state dynamical behaviors within which we can distinguish four main types (Figure 2):

- fixed point: for $a = 2$, the system is constant,
- periodic regime: for $a = 3.3$, the system oscillates between two fixed values,
- two-period regime: for $a = 3.5$, the system oscillates between four distinct values,
- chaotic regime: for $a = 4$, the system displays no periodicity and oscillates chaotically.

The logistic map application presents a series of behaviors controlled by the value of parameter a, from the stable point to a chaotic behavior.

This example leads us to explain the term chaos. This term, as well as the adjective "chaotic," denotes the combination of these properties: determinism, high sensitivity to initial conditions, and pseudo-randomness. This type of behavior occurs under certain conditions in highly non-linear systems.

Determinism: The chaotic series that we study represent the time evolution of a given set of variables. These evolutions are controlled by well defined physical principles, making possible the determination of the governing equations of motion for the system under study. Chaotic systems are controlled by an underlying determinism that sets their time evolutions.

Sensitivity to initial conditions: This property of chaotic systems was rediscovered by Edward Lorenz while studying certain aspects of climate modeling. In 1961, he was studying a differential system with three degrees of freedom. When rerunning a set of measurements, to save computer time, Lorenz started at half the sequence. He input as initial

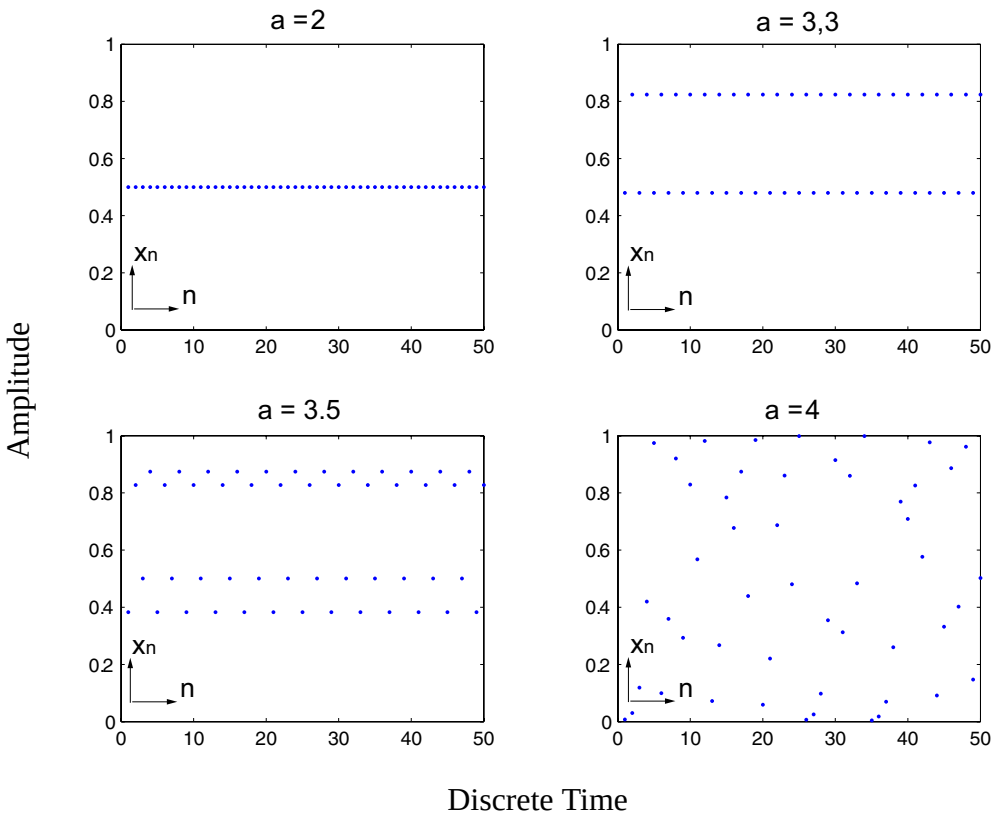


Figure 2: Discrete time traces of the logistic map application for different values of the control parameter *a*.

conditions those he had computed previously and printed. Much to his surprise, the results of these two series quickly diverged. The difference between the two time-series was that the computer used six decimal places, whereas the printer only printed up to three decimal places. Therefore, there was a slight difference in the initial conditions from which the two series were calculated.

From a practical perspective, this slight variation in initial conditions could be explained by an infinitesimal perturbation (noise) or by insufficient precision in the measurement of the initial state. Since the necessary precision could not be obtained for actual climate conditions, Lorenz concluded that climate could not be predicted for the long term. He had these famous words, often summarized by as "butterfly effect": "The flapping of a butterfly's wings, today in Peking, creates air turbulence that can transform into a storm tomorrow in New York" [38]. Lorenz studied several types of ordinary difference equations

and demonstrated that with as little as three non-linear coupled equations, a system could present this property of sensitivity to initial conditions [66].

We see that a very slight variation in initial conditions can generate important changes in the future evolution of the system. Chaotic dynamics, therefore, present a characteristically high sensitivity to initial conditions.

Pseudo-randomness: Pseudo-randomness is also referred to as unpredictability. Briefly, this unpredictability confers qualitatively to chaotic signals properties close to those of noise: no measurable periodicity, the presence of fluctuations on different time scales, and apparent disorder and unpredictability of the evolution. These properties can be characterized using tools such as spectral plots, autocorrelation, and probability density.

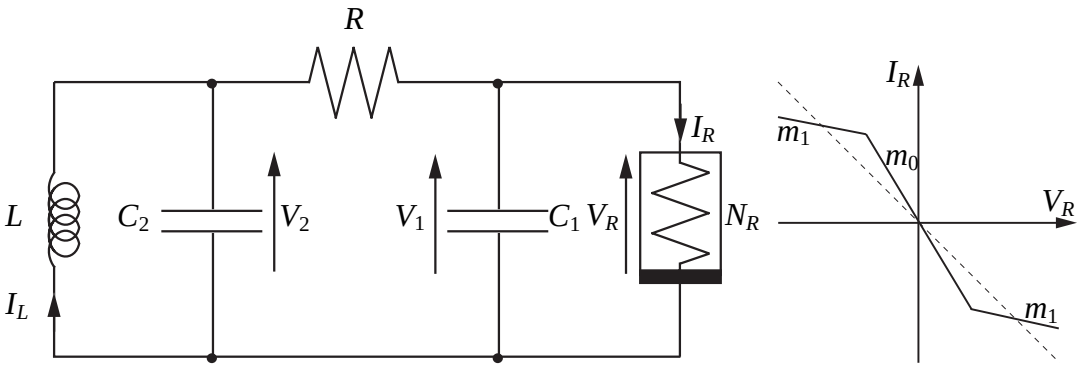
To summarize, a chaotic behavior can occur in differential (or in iterative) dynamical systems subject to strong non-linear components. When a chaotic state is achieved, the characteristic properties presented above are present: pseudo-randomness and sensitivity to initial conditions. These properties have led to using chaotic systems for cryptographic communication systems, detailed in section 2.1.2 and illustrated with the much studied electronic circuit called Chua's circuit [51, 52].

2.1.2 Chaos analysis tools

The properties described in section 2.1.1 can be clearly illustrated on Chua's circuit. In 1983, during a trip to Japan, Leon Chua witnessed an unsuccessful attempt to generate a chaotic dynamic with an electronic circuit based on the Lorenz equations.[1] This observation spurred him to develop his own electronic circuit [18]. Very quickly, the chaotic behavior of this circuit was demonstrated through both numerical simulation [67] and experiments [103].

Chua's circuit is a simple electronic circuit composed of resistors, capacitors, and inductors, as well as a fundamental non-linear element termed "Chua's resistance." This circuit is represented in Figure 3(a).

[1] The Lorenz equations are given in any chaos textbook, such as [12].



(a) Chua's circuit.

(b) Chua's non-linear resistance.

Figure 3: Chua's circuit and non-linearity.

The non-linear resistance can be obtained with two operational amplifiers and some resistors. The result is a piece-wise linear function that expresses the voltage V_R as a function of the current I_R, as shown in Figure 3(b). The equation of this function is:

$$I_R = g(V_R) = m_1 V_R + \frac{1}{2} \cdot (m_0 - m_1)\,[\,|V_R + 1| - |V_R - 1|\,] \tag{8}$$

By properly applying Kirkoff's voltage and current laws to the circuit, we can write three characteristic differential equations for this circuit. These equations link the three independent variables V_1, V_2 and I_L:

$$C_1 \frac{d}{dt} V_1 = \frac{1}{R}(V_2 - V_1) - g(V_1) \tag{9a}$$

$$C_2 \frac{d}{dt} V_2 = \frac{1}{R}(V_1 - V_2) + I_L \tag{9b}$$

$$L \frac{d}{dt} I_L = -V_2, \tag{9c}$$

with g defined by equation (8). The study of the dynamical regimes present in such a circuit is presented in [51], as is the study of the chaotic regime through the circuit's bifurcations and route to chaos as a function of the parameter R of Figure 3(a) [52].

Chua's circuit and associated governing equations serve as illustrations for the following chaotic dynamic analytical tools:

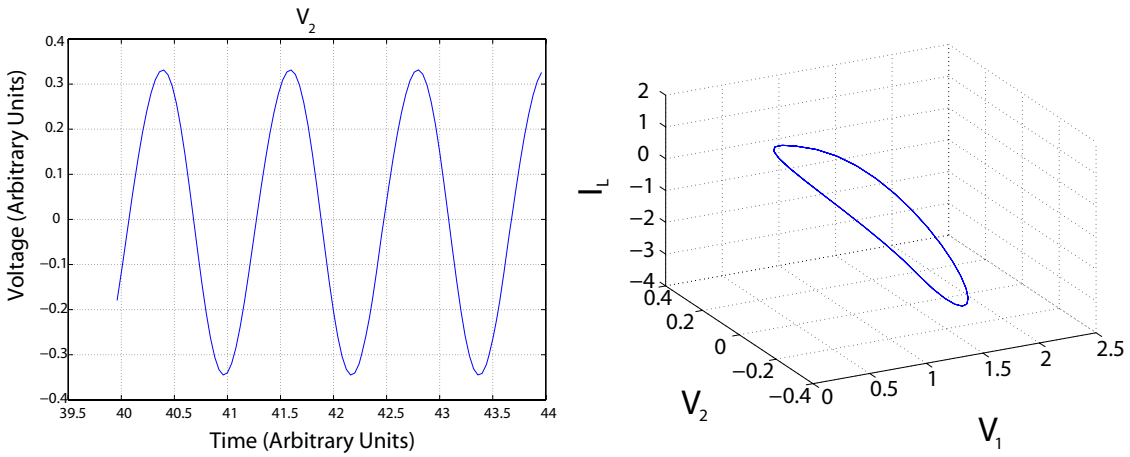
- Attractor trajectory in phase space,

- Chaos complexity through spectral analysis and autocorrelation function, and

- Determinism based on the precise route to chaos as represented by a bifurcation diagram.

2.1.2.1 Phase space

So far, we have mostly looked at the time evolution of chaotic dynamics. Yet, in some instances, dynamics may require analysis beyond their time dependence. The phase space describes the state evolution of the independent dynamic variables without the time reference. Each variable in the phase space represents a degree of freedom for the system. The graphic showing the dynamic trajectory in this space represents the attractor of the system. Each dynamic regime of a system is associated with a different attractor shape. For example, the attractor associated with a stationary regime is a point while the one associated with a periodic dynamic is a closed curve. As an illustration, a periodic time evolution and the corresponding attractor for Chua's circuit with $L = 22$ mH are presented in Figure 4.



(a) Time trace.

(b) Phase space trajectory.

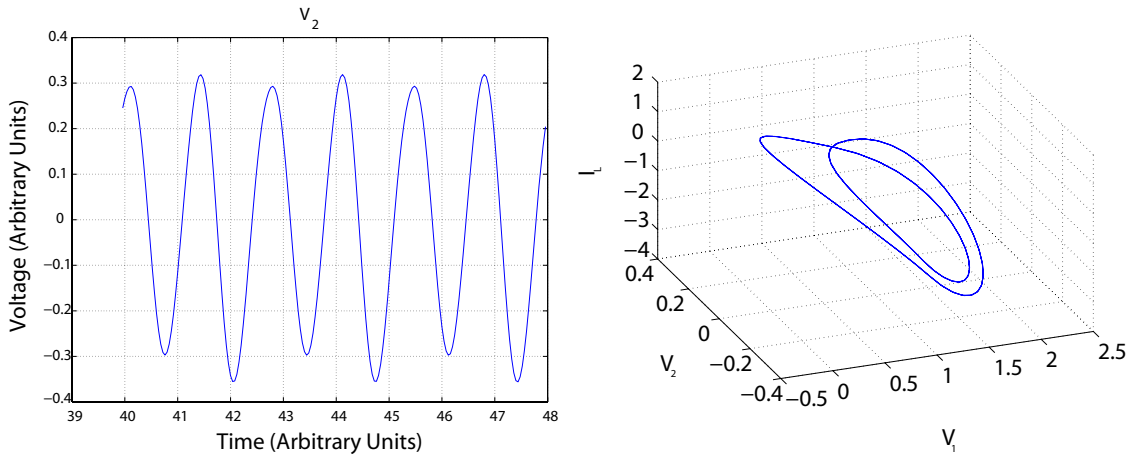
Figure 4: Chua's Circuit in periodic regime with $L = 22$ mH.

Values for the parameters of the circuit used in Figure 4 (modeled by equations (8)

and (9)) are typical for this circuit and are given by:

$$\begin{aligned} C_1 &= 10nF \\ C_2 &= 100nF \\ R &= 20\Omega \\ m_0 &= -\frac{8}{7} \\ m_1 &= -\frac{5}{7} \end{aligned} \tag{10}$$

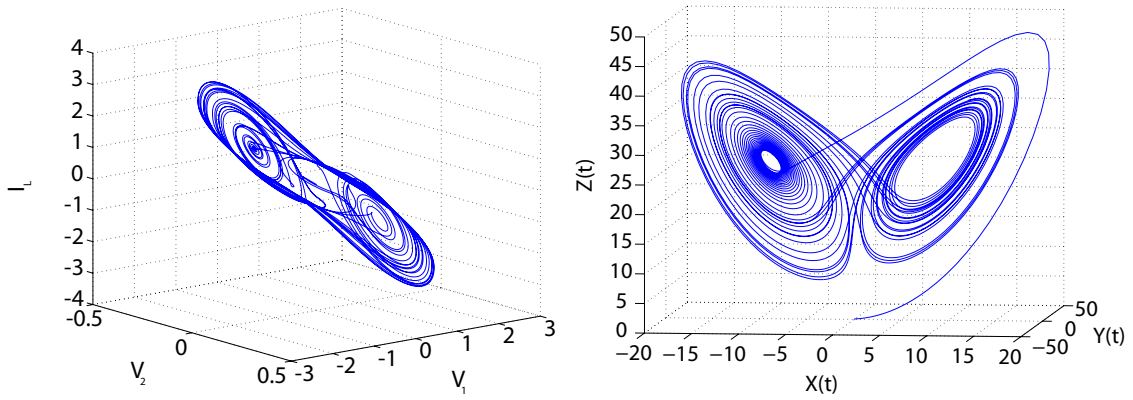
A periodic regime of higher complexity is obtained by increasing the value of the parameter L of Equation (9). We then observe the presence of two frequencies, corresponding to a different attractor. Indeed, the shape of this attractor corresponds to a figure '8', as illustrated in Figure 5.



(a) Time trace. (b) Phase space trajectory.

Figure 5: Chua's circuit in a two period periodic regime with $L = 28$ mH.

Further increasing the control parameter L brings the system to a chaotic regime. The attractor in the phase space takes a shape characteristic of Chua's circuit: the "double scroll," as shown in Figure 6(a). For comparison, the "butterfly wings" characteristic attractor of the Lorenz equations is shown in Figure 6(b). We clearly see a difference in the overall shape of the two attractors, illustrating the distinct nature of each attractor.



(a) Chua's attractor - $L = 43mH$.

(b) Lorenz's attractor.

Figure 6: Chua's and Lorenz's attractors.

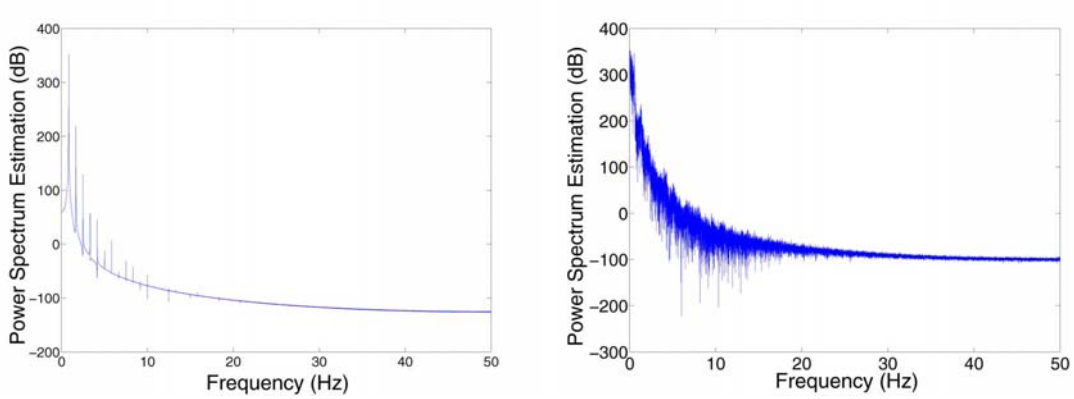
2.1.2.2 Spectrum and autocorrelation

As we have seen in the previous section, proper values of control parameters generate chaotic system behavior. One way to characterize a chaotic signal is to compute its frequency spectrum and autocorrelation. The frequency spectrum, obtained using the Fourier transform, is computed as a function of the time trace by the following relation involving the two reciprocal variables time t and frequency f:

$$\tilde{X}(f) = \int_{-\infty}^{+\infty} x(t)\, e^{-2j\pi f t}\, dt \tag{11}$$

The Fourier transform $\tilde{X}$ is complex. The modulus of this quantity represents the magnitude spectrum and the argument, the phase spectrum. For our proposed research, we are only interested in the magnitude spectrum and the power spectrum estimation, $|\tilde{X}(f)|^2$. Since the chaotic observable of our research will be an optical intensity, using the magnitude spectrum and power spectrum estimation is appropriate.

We see in Figure 7(a) the power spectrum estimate for Chua's circuit in the periodic regime. The corresponding time trace and attractor are shown in Figure 4. The spectrum shows lines at the fundamental oscillating frequency and at the harmonics. The spectrum of the chaotic oscillations of Chua's circuit is shown in Figure 7(b), corresponding to the attractor of Figure 6(a). The spectrum of the system in the chaotic regime shows a continuum of frequencies present, and not a set of discrete lines as for the periodic case. The



(a) Periodic regime. (b) Chaotic regime.

Figure 7: Magnitude sprectra of Chua's circuit in periodic and chaotic regimes.

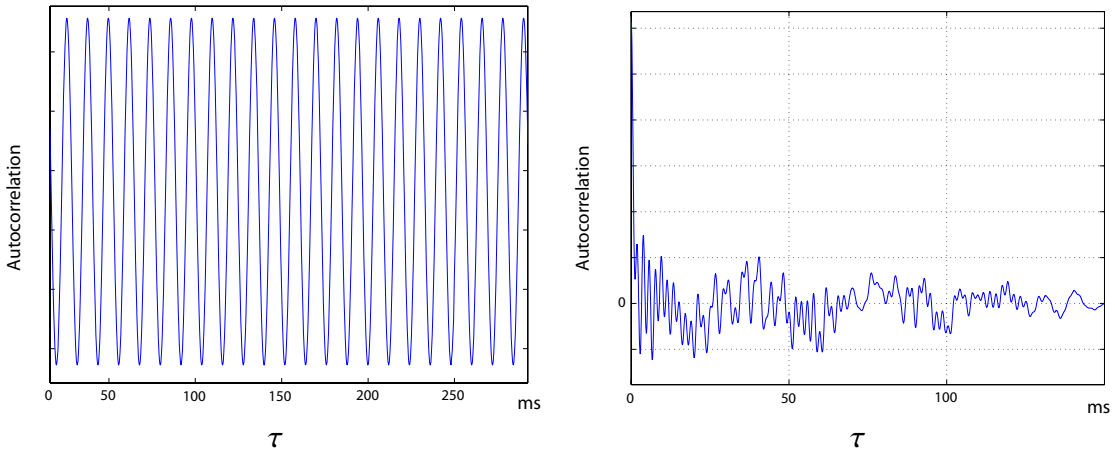
frequency continuum is an indication of a great richness in the dynamics.

The power spectrum estimation is the Fourier transform of the autocorrelation function, as stated by the Wiener-Kintchine theorem [12]. The autocorrelation function is defined as

$$C(\tau) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} X(t) \cdot X(t+\tau)\, dt. \tag{12}$$

This function measures the resemblance of the signal X, at a given time t, with values of X at a subsequent time $t+\tau$. By varying τ, we can construct the function $C(\tau)$ that quantifies the time self-similarity of the signal. If the signal $X(t)$ is constant, periodic or quasi-periodic, then $C(\tau)$ will not tend to zero as τ tends to infinity because the spectrum will be composed of discrete lines. Periodic (or quasi-periodic) signals conserve their internal self-similarity as time flows. Indeed, the system behavior is predictable, since knowledge of the time evolution during a sufficient time period provides complete knowledge for all subsequent times. In the case of the chaotic regime, $C(\tau)$ drops to zero as τ increases, as illustrated in Figure 8.

Figure 8(a) clearly shows a periodic autocorrelation function for a periodic signal. This autocorrelation function is to be compared with the autocorrelation function of the chaotic regime, presented in Figure 8(b). The autocorrelation of the chaotic signal starts high for τ close to 0 and then decreases very rapidly as τ increases. Knowledge of the chaotic signal $X(t)$ for any given time frame does not allow reliable prediction on the future evolution of



(a) Periodic regime. (b) Chaotic regime.

Figure 8: Autocorrelation of Chua's circuit in periodic and chaotic regimes.

$X(t)$.

2.1.2.3 Bifurcation diagram

A non-linear dynamical system can behave differently depending on the system's parameter values, as we have seen for Chua's circuit. Different behaviors include periodic, quasi-periodic and chaotic regimes (Figure 2). A system transitions from one type of behavior to another depending on the value of a set of important system parameters. These regime transitions occur via a bifurcation process; the parameters responsible for these regime changes are called bifurcation parameters. The complete dynamic evolution of a system can be represented by a bifurcation diagram.

Graphical representations of the bifurcations can be conducted in several ways. The one we chose places the considered bifurcation parameter on the abscissa axis and the time amplitude of the dynamic variable on the ordinate axis. Color coding represents the probability density function (PDF) of the ordinate amplitudes.

Multiple ways exist for a dynamical system to progress from one regime to another as the bifurcation parameter is increased. This progression is often termed the "route to

chaos". For the logistic application (Equation (7)), this route is a cascade of period doubling.[2] This bifurcation cascade is an infinite sequence of periodic regimes from a point to a second order cycle (2 values are images of each other by the logistic application f), a cycle of order $4 = 2^2$ (4 values are images with respect to $f \circ f$), from an eighth order cycle (images for $f \circ f \circ f \circ f$), ... up to infinite length cycles 2^n ($n \to \infty$) which are observed up to a finite value of the bifurcation parameter, called accumulation point a^*. Past this point, we observe an inverse cascade of chaotic regimes with each of these regimes corresponding to a periodic sequence of intervals of chaotic values. This period is 2^n, where n decreases from infinity at $(a^*)^+$ to 0. When $n = 0$, we have fully developed chaos. For $a > a^*$, we also observe periodic regimes within periodic windows with these regimes also evolving towards chaos by a doubling cascade.

Based on the logistic application, the bifurcation diagram of Figure 9 illustrates the "route to chaos." This diagram presents the normalized probability density function (color coded) as a function of the bifurcation parameter and the amplitude of the oscillations. The zone of the fixed point (on the left hand side of the figure) and the zone of chaotic oscillations (completely on the right hand side of the figure) can both be distinguished. Between the two, for values of a in the interval $[3; 3.6]$, we observe the cascade period doubling of the initial periodic regimes. After $a^* \approx 3.57$, we observe the emergence of chaotic regimes (i.e. a dense PDF over intervals).

In Figure 9 we can clearly see the four separate oscillation types. The stable system regime is distinctly visible on the left of the diagram, and the chaotic regime on the right of the figure. A first bifurcation occurs around $a = 3$ and we can clearly see the periodic regime. As a increases, another bifurcation occurs: the system enters the two-period regime.

The practical use of bifurcation diagrams in chaos cryptography is to identify the parameter values that lead to chaotic oscillations of our dynamic system. The study of the

[2] Other typical routes include intermittence and quasi-periodicity [12]

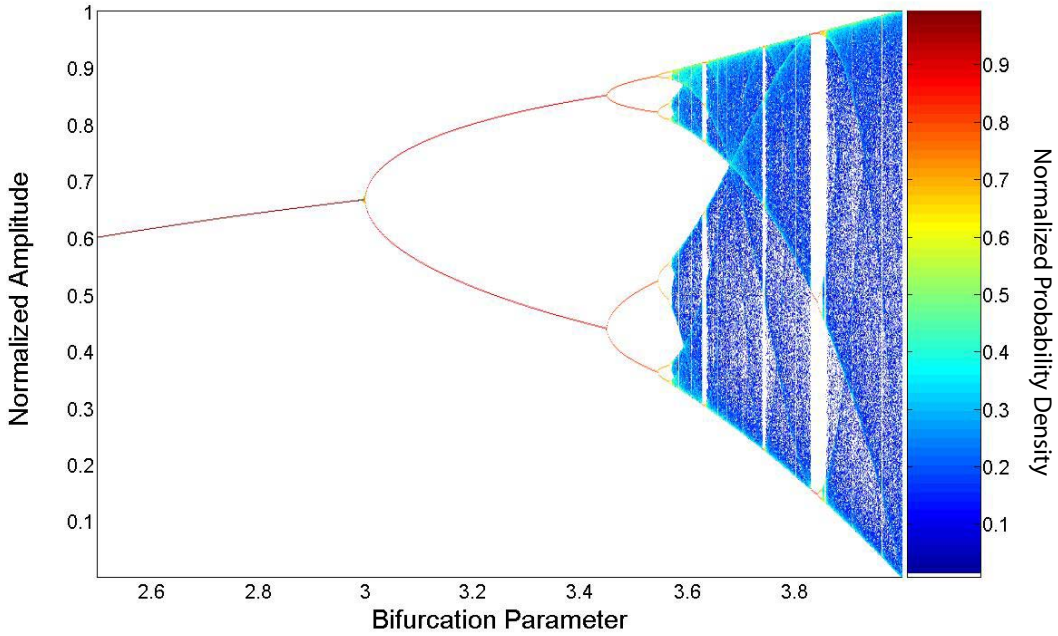


Figure 9: Bifurcation diagram of the logistic map.

experimental bifurcation diagram of our chaos generator will be in Section 3.2.2.3.

2.2 Chaotic system properties applied to secure communications

In the previous sections, we detailed fundamental properties (e.g. unpredictability, sensitivity to initial conditions) of chaotic systems and presented various tools (such as power spectrum estimation and the bifurcation diagram) to analyze and characterize these systems. We will now link chaotic systems and communications by explaining how specific properties of chaotic systems make them appropriate for secure communication.

We first examine the property that makes chaos communication possible, before examining other properties of chaos that allow extension from communication to secure communication.

2.2.1 Chaotic system properties applied to communications

The key word used to describe the phenomenon that enables two chaotic systems to communicate is called synchronization. Chaotic synchronization was first evidenced in the

works of Pecora and Carroll [77].

In this section we explore the relationship between two signals, $x_1(t)$ and $x_2(t)$, produced by two distant non-linear dynamic systems. These two systems are unidirectionally coupled. The objective of this coupling is to force the two distant chaotic signals to exhibit identical properties. We are especially interested in complete synchronization. This form of synchronization can be expressed by $x_1(t) \equiv x_2(t)$ at t_∞ or $\lim_{t\to\infty} |x_1(t) - x_2(t)| = 0$. In other cases, partial synchronization of components of these signals is possible, for example, their phases, $Arg[x_1(t)] = Arg[x_2(t)]$, as presented in [90].

The link between the two signals that allows for their synchronization is termed coupling. This coupling can be implemented in different ways. Unidirectional coupling, the implementation we have chosen for this work, corresponds to the classic "master-slave" synchronization scheme where the slave signal is expected to faithfully follow the master signal. The master system is called the "emitter" and the slave system the "receiver." Synchronization phenomena can also be observed for bidirectional couplings.

An important characteristic of the coupling is the coupling ratio c, also called the coupling coefficient (as illustrated in Equation (13)). This coefficient typically varies between 0 and 1. When $c = 0$, there is no coupling and the emitter and receiver oscillate separately. In the case where $c = 1$, the coupling is total. This case corresponds to the complete control of the slave by the master. For intermediate values of c, there exists a threshold for c beyond which we can observe synchronization phenomena. Below this limit, the master-slave synchronization is not effective.

Going back to the dynamical system described by Equation (1) and restricting ourselves to the one-dimension case where the emitter variations are then described by $\frac{x_1(t)}{dt} = F_1(x_1)$, the variations of the receiver are then given by:

$$\frac{x_2(t)}{dt} = F_2[x_2 + c \cdot (x_1 - x_2)]. \tag{13}$$

When the initial conditions are identical and when $x_1 \equiv x_2$, we obviously observe a case of complete synchronization when $F_1 \equiv F_2$, independent of the value of c.

In the previous description, the problem of synchronization stability was not discussed. Indeed, in the presence of noise, or some other perturbation, the two systems, initially synchronized, can lose synchronization. Pecora and Carroll looked at the problem in the following manner: they decomposed the dynamical system into sub-systems that interact with one another. They showed that a receiver composed of a set of these subsystems was able to produce chaotic signals stably synchronized under certain conditions. These conditions concern the properties of conditional stability with respect to the rest of the system. This relative stability was measured with conditional Lyapunov exponents, also called sub-Lyapunov exponents [77]. With this particular coupling scheme and with this sub-system decomposition Pecora and Carroll were the first to demonstrate chaotic behavior synchronization. Their work was based on previous theoretical studies [32] and experimental work [95].

This synchronization using the sub-system decomposition scheme has been studied experimentally with Chua's circuits [54, 74] and on Lorenz's systems [21, 22, 39]. To illustrate this approach, we go back to the example of Chua's circuit from Section 2.1.2. One example used the circuit shown in Figure 3 as the emitter and the one shown in Figure 10 as the receiver. The coupling is realized between those two circuits by the voltage V_{C1} of the emitter. This signal from the emitter goes through a voltage follower operational amplifier before completing the coupling with the receiver circuit. The received signal coupling is then called $r(t)$.

The receiver is divided into two sub-systems clearly indicated in Figure 10. These two sub-systems are linked by a voltage follower operational amplifier to force the unidirectionality of the coupling. The first sub-system comprises the capacitor C_2, the resistance R, and the inductance L. The second sub-system is formed by the resistor R, the capacitor C_1, and Chua's resistor N_R.

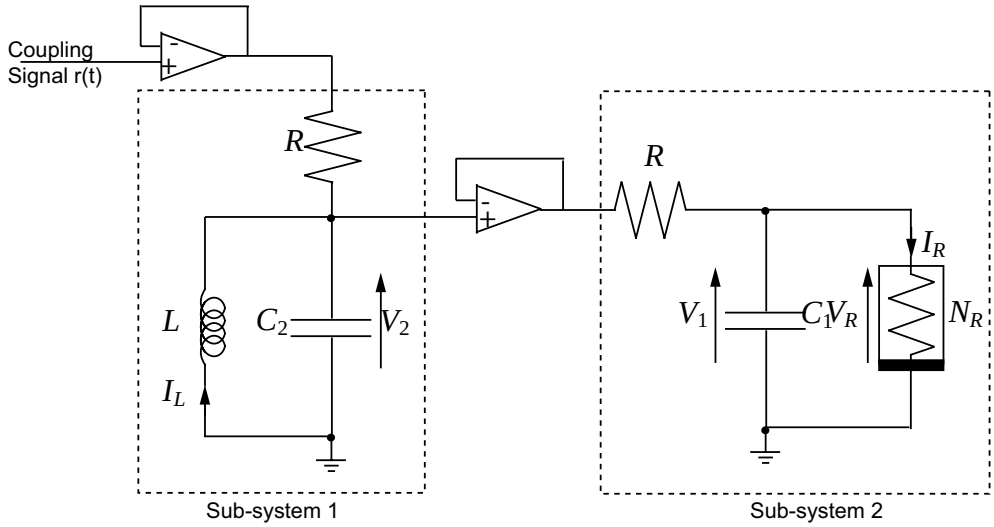


Figure 10: Chua receiver decomposed into sub-systems.

The behavior of the first sub-system "*RL*" of the receiver is described by the two equations:

$$C_2 \frac{d}{dt} V_2 = \frac{1}{R}(r(t) - V_2) + I_L \tag{14a}$$

$$L \frac{d}{dt} I_L = -V_2, \tag{14b}$$

The voltage V_1 controls the second sub-system "*RC*," whose behavior is given by

$$C_1 \frac{d}{dt} V_1 = \frac{1}{R}(V_2 - V_1) - g(V_2). \tag{15}$$

When the values of the electronic components and Chua's resistance are the same for both emitter and receiver, we can observe a synchronization phenomenon. Indeed, voltage V_1 of the receiver synchronizes with voltage V_1 of the emitter,[3] and both voltages present the same time evolution.

From these two synchronized Chua's circuits, message transmission has been achieved, both for analog [54] and digital [74] messages. We now investigate how chaotic systems can be used to provide communication security.

[3]We have not introduced a different set of notations for emitter and receiver variables or parameters.

2.2.2 Extension to secure communications

Numerous communication systems are based on the synchronization of harmonic carrier waves. Both AM and FM radio are examples of such systems. Because of the synchronization property shown above, we can envision chaotic signals being used as carrier waves in communication systems. Using properties specific to chaotic signals, communication systems with chaotic carrier waves can also offer communication security.

Chaotic signals are highly broadband signals with noise-like characteristics and high unpredictability as a result of their sensitivity to initial conditions. This noise-like characteristic is precisely the element bringing security to the communication. The message encoding principle at the emitter consists of masking the message in the chaotic signal. This technique can be likened to jamming a signal to prevent its proper detection and decoding (for example, the jamming of the BBC by the Germans during the second World War).

In our case, the jamming is clearly intended to prevent the unwanted detection of the secret message. With synchronization capability, the authorized receiver is able to filter out the chaotic carrier and extract the message from the transmitted signal. Because of the sensitivity to initial conditions, a precise knowledge of the chaos parameters, which serves as the cryptographic key, is necessary to properly synchronize and decode the message.

From the previous description, one can see that the choice of a chaotic signal is important to the quality and efficiency of the masking. The closer to noise the chaotic signal is, the more efficient the masking is. Many techniques exist for generating a chaotic signal. Indeed, the first electronic demonstrators of chaos cryptography were based on the Lorenz's circuits [73] for which, although wideband, a spectrum plot clearly shows characteristic frequencies. This initial attempt at a cryptographic system was quickly broken using a parametric identification technique on the chaotic carrier wave [55, 75].

To be applicable to modern telecom techniques, chaos cryptography systems must follow the rapid development of optical networks, both in data rates and in capacity. They

also need to include the latest developments in network protocols in order to be deployable. Therefore, chaos cryptography systems must have wideband properties to properly encrypt the multi-GHz signals that are the norm in optical networks. They must also be compatible with the existing network architecture.

2.2.3 Cryptography within telecom networks

Current network point-to-point communication is controlled by a set of protocols that operate at different levels of the network stack. To understand the proper positioning of the system we propose, let us look at the seven layers of the OSI model (Open Systems Interconnection), as developed by the ISO (International Organization for Standardization). This international organization, dependent of the United Nations, defines international standards in domains other than electricity and electronics. The OSI model was developed as a seven layer protocol stack (Figure 11). Each layer plays a particular role in enabling com-

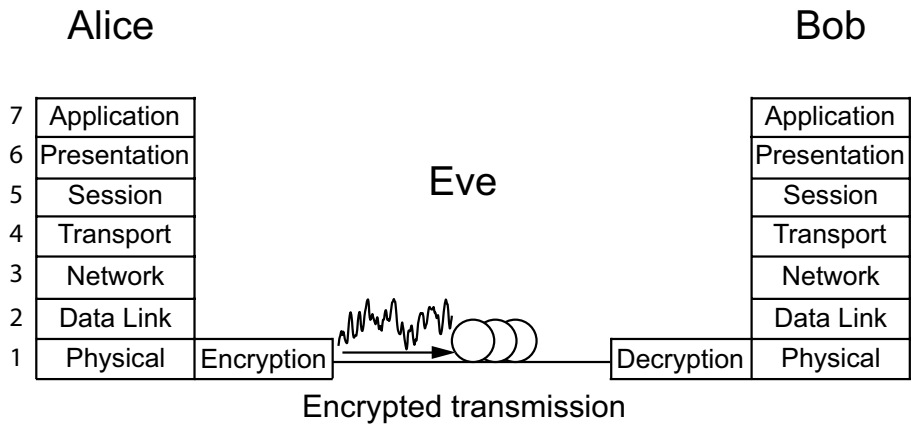


Figure 11: Seven layer OSI model.

munication between distant systems [70]. We will limit ourselves to a point-to-point link within a network. During the rest of this dissertation, we will refer to the emitter as Alice and to the receiver as Bob. Eve is the spy that listens to the communication channel. Without going into the functional details of each layer, layers 7 to 4 pertain to communication and routing of the message from source to destination. Layers 3 to 1 handle the network access and the transmission of the message according to the route determined by the upper

layers.

The proposed security takes place directly at the physical layer of the OSI stack. Since classical algorithmic cryptography methods are implemented typically at the application layer, the transparency of the encryption we propose allows the simultaneous use of both algorithm based and chaos cryptography. Another advantage is the compatibility of this method with wavelength division multiplexing (WDM) networks, as detailed below.

We limit ourselves to the case of a unique transmission channel. Modern techniques exploit one of the principal advantages of optical fiber: its great bandwidth. Wavelength Division Multiplexing (WDM) enables the transmission of multiple channels within the same fiber; each channel being defined by the wavelength of its carrier wave. The chaos cryptography technique encrypts a given WDM channel. Each channel, encrypted or not, is then part of the WDM network as illustrated on Figure 12. Multiple signals using carrier waves of different wavelength are injected into the same fibre through a multiplexer (MUX). At the other end of the fiber, the different wavelengths are separated by a demultiplexer (DEMUX). The information carried by each signal can then be detected separately.

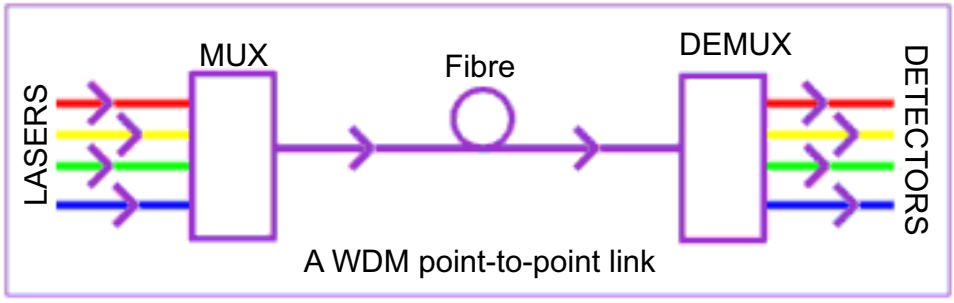


Figure 12: Schematic diagram of a point-to-point WDM link.

Since current optical networks are exclusively WDM based and our encryption method is compatible with WDM technology, we can envision combining chaos cryptography with current network protocols. These network protocols are undergoing an evolution. They are distancing themselves from the OSI stack with layers 2 and 3 merging their functionalities

(routing and switching). This evolution is beneficial to the integration of chaos cryptography within optical networks.

The objective of MultiProtocol Label Switching (MPLS) is to optimize the operations of layers 2 and 3 by combining them. The aim is to avoid unnecessary encapsulation of packets due to deployment of redundant protocols on different layers. The "MultiProtocol" aspect stems from the necessity for compatibility with all the protocols deployed on the Transport level. The solution implemented by MPLS calls for the use of labels. A label, is assigned to each packet based on its next hop. At each node, the label is analyzed and the packet is directed towards its next hop, until it reaches its destination. Figure 13 presents an example of the workings of an MPLS network operation.

The necessity of analyzing the packet (specifically the label) at each node slows down considerably the progression of a packet within a network, especially an optical network since opto-electronic conversions are required at each node. These conversions pose an additional problem at the hardware level. Encryption and decryption systems need to be present at each node, greatly increasing the cost and complexity associated with deploying chaos cryptography on a full scale network.

To circumvent the opto-electronic conversions, an other type of label was developed, specifically for optical networks. Instead of coding the label electronically as part of the packet, the wavelength of the transmission serves as the label. The signals are now switched at each node according to their incoming wavelength. This specific implementation of MPLS is called MPλS.

In Section 2.3, we will discuss the integration of the cryptographic system we are proposing within MPλS networks and we will extend the security of the our cryptographic scheme over the end-to-end communication.

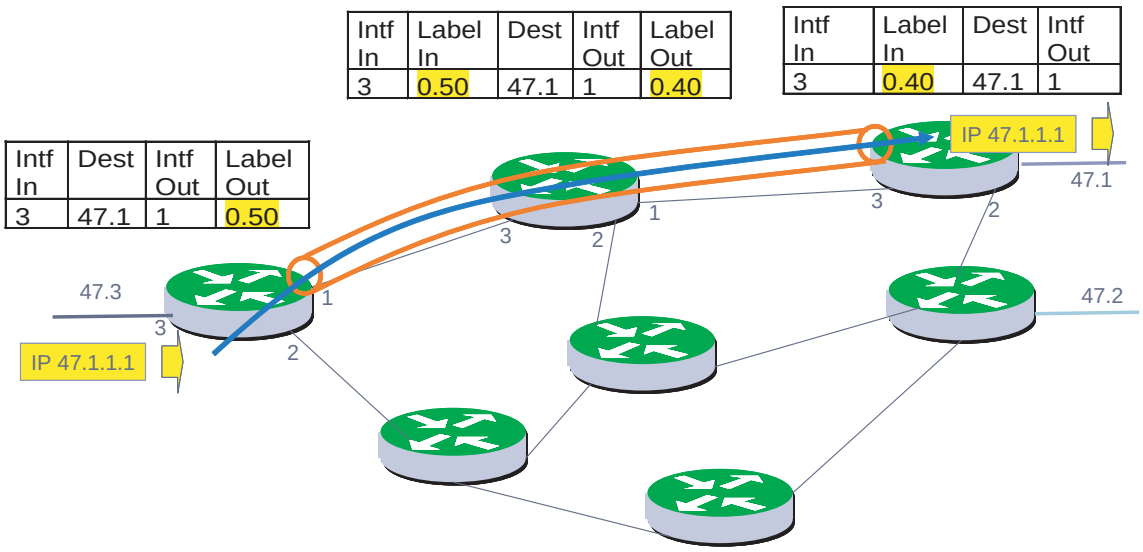


Figure 13: Message transmission through an MPLS network.

2.3 Experimental optical chaos cryptography

Current telecom systems implement, at a minimum, optical SONET OC-192 (10Gb/s) rates.[4] Electronic systems, such as Chua's circuit, cannot match these bit rates and, therefore, cannot implement real-time encryption at current bit rates. Thus, novel systems with much wider bandwidths have been developed.

The solution to this bandwidth problem is to exploit the naturally wide bandwidth of optical fiber and the emitter/receiver systems that they are associated with. Working with signals in the telecom C band (centered around the 1550 nm telecom window) provides a certain level of compatibility with existing telecom systems.

The different chaos cryptography systems for optical networks can be classified by their chaos generation techniques. In this section, we distinguish the family of all-optical chaos generators from the opto-electronic ones. We also categorize systems based on their underlying dynamical process and associated modeling: rate equations (such as Lang-Kobayashi) or electronic filtering equations.

[4]For a complete list of OC rates, see [70].

2.3.1 All-optical systems

Under the broad category of "all-optical" systems, two principal schemes have been implemented for generating chaotic carriers to use for chaos cryptography. The first scheme has a laser injecting its light into another semiconductor laser. The second scheme uses optical feedback to induce chaotic behavior [64].

2.3.1.1 Injection laser

Let us first investigate the case of a semiconductor laser subject to some optical injection, according to the diagram of Figure 14. An optical signal of constant amplitude E_s and of frequency ω_s from the master laser is injected through an optical isolator and an attenuator of coefficient K into a monomode slave laser. The envelope of the electric field $E(t)$ at the output of the slave laser is E_0.

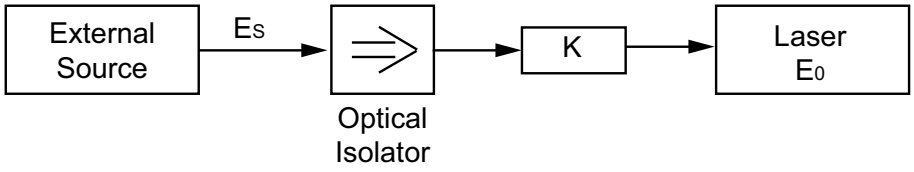


Figure 14: Coupling by injection in between two laser sources.

The behavior of this kind of system can be modeled by the Lang-Kobayashi equations [56], taking into account the forcing term from the optical injection [88]. The electrical field injected by the external source into the slave laser is expressed as $E_s e^{j\omega_s t}$. Let $E(t) = E_0(t)e^{j[\omega t+\phi(t)]}$. We then write separately the equations for amplitude E_0, phase ψ, and population inversion density N:

$$\frac{dE_0}{dt} = \frac{1}{2}\left\{G_n(N-N_0)(1-\epsilon\Gamma E_0^2) - \frac{1}{\tau_p}\right\}E_0 + \frac{K}{\tau_{in}}E_S\cos\psi(t) \tag{16a}$$

$$\frac{d\psi}{dt} = \frac{1}{2}\,a^*\left\{G_n(N-N_0)(1-\epsilon\Gamma E_0^2) - \frac{1}{\tau_p}\right\} - \frac{K}{\tau_{in}}\frac{E_S}{E_0(t)}\sin\psi(t) - \Delta\omega_S \tag{16b}$$

$$\frac{dN}{dt} = Rp - \frac{N}{\tau_r} - G_n(N-N_0)(1-\epsilon\Gamma E_0^2)E_0^2. \tag{16c}$$

The parameter τ_{in} represents the system dynamic characteristic time, given as $8 \cdot 10^{-12} s$, $\Delta\omega_s$ is the phase difference between the internal and the injected fields, G_n is the modal gain, N_0 is the carrier concentration at the inversion threshold, $\epsilon\Gamma$ is the product of the compression and the confinement factors, τ_p is the photon lifetime in the cavity, τ_r is the electron/hole recombination time, $R_p = J\eta/ed$ is the pump parameter that depends on the supply current density J, the efficiency η, and the active region thickness d [7]. The integration of equations (16) gives the envelope E_0 time evolution of the electromagnetic field E. The bifurcation parameter is the value K, which controls the attenuation of the field E_s injected into the slave laser. This parameter controls the nature of $E_0(t)$'s dynamic.

Two types of system dynamics can be separated into two different regimes based on the value of K (hence the injection level): the weak injection regimes and the medium injection ones. As K increases, starting at 0, the system goes through multiple bifurcations as it transitions from a stable regime to periodic oscillations with an increasing number of periods, before lapsing into chaotic oscillations. Above a certain injection level, the system presents a cascade of inverse bifurcations before the envelope E_0 stays constant [7]. The laser with optical injection is a method to generate a chaotic variable by varying the injection level of the master laser to the slave laser.

A more complete subsequent study of the same system showed evidence of the presence of five distinct zones of behavior for the laser within the model schemed in Figure 14. The two parameters that vary are now the injection level K and the difference $\Delta\omega_s$ between the optical frequencies of both lasers, ω_s and ω_0. As a function of these parameters, the slave laser is in one of these five zones:

- The phase of the slave laser can lock onto that of the master laser. The dynamical variables that characterize the system reach constant values.

- The intensity of the slave laser is modulated at $\Delta\omega$.

- The field of the slave laser oscillates at its relaxation frequency.

- The oscillations become chaotic after many frequency doublings.

- The phase of the slave laser fluctuates greatly.

The knowledge of these two parameters and their proper setting can force the slave laser into its zone of chaotic oscillation, thus providing a suitable chaos generator for wideband chaos cryptography [9].

For the system we have just studied, the forcing signal was provided by a laser external to the dynamical system under consideration. The laser's own signal can be used via optical feedback as the forcing signal.

2.3.1.2 External cavity laser

The optical feedback of the laser on itself is equivalent to coupling an external cavity. Chaotic oscillations can also be observed with this type of setup. The external cavity can be termed short or long, depending on the cavity travel time.

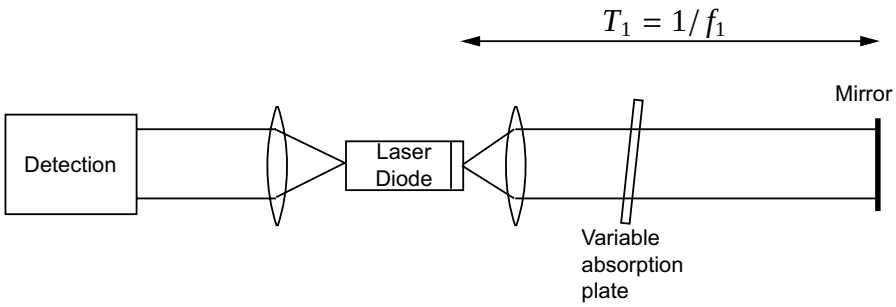


Figure 15: Semiconductor laser coupled to an external cavity of length T_1.

Figure 15 presents an example of a short cavity. The mirror at the end of the cavity reflects the light back into the inside of the cavity and, therefore, back into the laser. The nature of this cavity may vary; depending on the cavity length, we prefer an air or a fiber cavity.

A system implementing a bulk optics external cavity will be described first. The length of this cavity varies from 30 cm to 1.5 m, which corresponds to the modes of the external cavity for a free spectral range between 100 and 500 MHz. When varying the optical

feedback strength K by adjusting the variable absorption plate, the system changes dynamical states. By increasing K, the system oscillates chaotically after a period doubling cascade [28].

The dynamical system described previously is modeled by the equations governing the electrical field E, the population inversion N of the laser, again following the proposed model by Lang and Kobayashi [56], presented here in its complex form:

$$\frac{d\tilde{E}_0}{dt} = \left\{ i\omega(N(t)) + \frac{1}{2}[G(N(t)) - \Gamma] \right\} \cdot \tilde{E}_0(t) + K \cdot \tilde{E}_0(t - T_1) \tag{17a}$$

$$\frac{dN}{dt} = P - \gamma_{\|} N(t) - G(N(t)) \cdot |\tilde{E}_0(t)|^2 \tag{17b}$$

$$G(N) = \Gamma + G_n(N - N_{tr}). \tag{17c}$$

In these equations, ω is the diode cavity longitudinal mode resonant frequency and T_1 the cavity transit time. The constant Γ is the cavity loss of the diode cavity, c represents the light velocity, and N represents the carrier density. P represents the number injection rate per unit volume of the exited carriers, which is related to current density J, electronic charge e, and the diode active layer thickness d as $P = J/ed$. The inverse spontaneous lifetime of the excited carriers is noted $\gamma_{\|}$. G is the system gain.

These equations closely describe the chaotic behavior of the physical system and confirm the presence of chaotic regimes. The Lyapunov spectrum, Kaplan-Yorke dimension, and Kolmogorov-Sinai entropy have been calculated for this case [94].

To explore a system with longer cavity lengths, the bulk optics must be replaced with a more convenient setup. With its flexibility and ease of use, optical fiber can successfully replace the bulk optics. The optical cavity now has a length L, according to Figure 16.

Experimental and numerical studies have shown that chaotic regimes are obtained for a larger range of values for the K parameter with greater cavity length [8]. In a cryptographic sense, this increase means that a greater number of keys is available to encrypt a message.

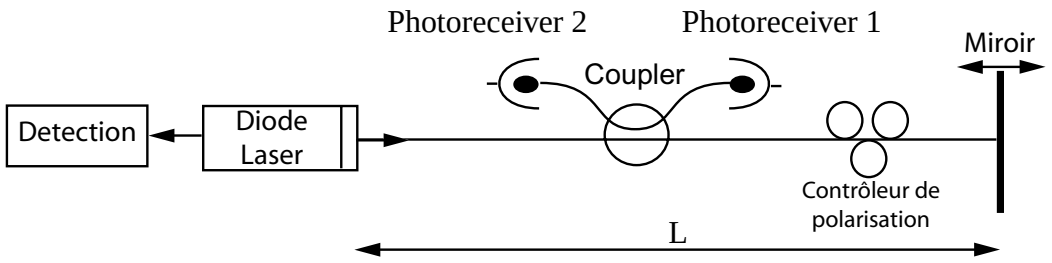


Figure 16: Semiconductor laser coupled to an external fiber cavity.

The two all-optical systems presented here can behave chaotically under certain identified conditions. The main setback of these systems is their sensitivity to optical phase. For a telecom application, to ensure better stability, any form of optical phase dependence should be removed. Therefore, a combination of optics and electronics has been developed, as detailed in the following section.

2.3.2 Transition towards an opto-electronic dynamic

Optical feedback systems take advantage of the very large bandwidth provided by optical fiber but are subject to constraints that affect their performance, in terms of reliability, stability, and mechanical robustness. These systems are especially sensitive to polarization and to optical phase. An alternative approach developed to overcome those problems combines electronics and optics in a feedback loop. The result is an opto-electronic oscillator [64]. The opto-electronic conversion by a photo-detector suppresses the system sensitivity to optical phase and polarization. In a sense, this approach, although presented as novel in [64], takes a step back in time, as experimental setups combining optics and electronics have already been studied [5, 71]. In both these cases, opto-electronic feedback systems have presented chaotic behavior over a certain parameter range. Another non-negligible advantage of opto-electronic systems is their flexibility. Indeed, the different parameters of the chaotic dynamic depend on component settings (optical power, delay length). Moreover, components are interchangeable with any other in order to better control the dynamic. This flexibility is not possible for all-optical systems whose parameters depend on the physical characteristics of a laser. These characteristics are fixed during the

fabrication process of the laser, but their control is often unprecise.

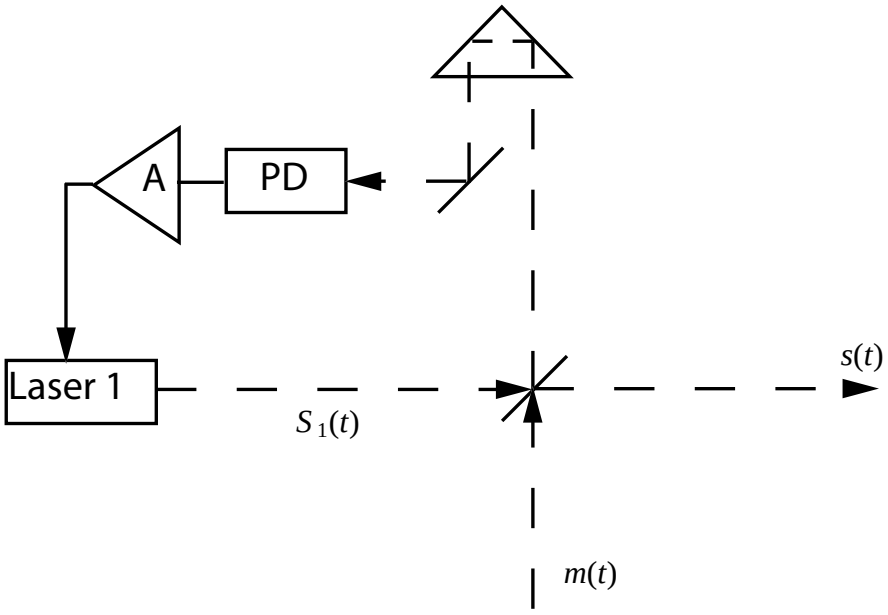


Figure 17: Experimental setup of the opto-electronic system.

The experimental setup of the emitter of a chaotic system with opto-electronic feedback is presented Figure 17. The signal output from the emitter laser is fed back through a combination of a photoreceiver ("PD" on the figure) and an amplifier (’A’ on the figure) to the injection current of the laser.

Since the photoreceiver reacts only to the variations of the optical signal intensity, neither the optical phase nor the polarization state are taken into account. The emitter can be modeled by the coupled equations of photon density and carriers:

$$\frac{dS_1}{dt} = -\gamma_c S_1 + \Gamma g S_1 + 2\sqrt{S_0 S_1} F_{S,1} \tag{18a}$$

$$\frac{dN_1}{dt} = \frac{J}{ed}[1 + \xi y_1(t-T)] - \gamma_s N_1 - g S_1 \tag{18b}$$

$$y_1(t) = \int_{-\infty}^{t} d\eta f_1(t-\eta)\frac{s(\eta)}{S_0}. \tag{18c}$$

N is the carrier density, η is the injection coupling rate, S is the amplitude of the injection field at an optical frequency ω_i. J is the injection current density, e is the electronic charge,

d is the active layer thickness of the laser, ξ is the injection parameter, γ_c is the cavity decay rate, γ_s is the spontaneous carrier decay rate, and g is the optical gain coefficient. S_0 is the free-running laser photon density at the given operating point, and F_s is a stochastic noise term. The '1' indices denote an emitter variable. T represents the delay linked to the propagation time through the feedback loop, and the function f_1 the normalized impulse response of the opto-electronic feedback. This chaos generator has an experimental spectrum of bandwidth 6 GHz [65].

2.3.3 Other opto-electronic chaos cryptography systems

We pursue our exploration of the diverse possibilities offered by opto-electronic feedback systems. In the previous section, we saw systems built around a semiconductor laser with opto-electronic feedback. We now detail different opto-electronic systems that each use a different variable (wavelength, phase, intensity...) for the chaotic dynamical process. Each of these systems shares the same type of limitation: the limitations of the dynamics are no longer the result of the laser limitations but are caused by a filter function of the opto-electronic feedback. Each system, with its different dynamic variable, has advantages and disadvantages.

2.3.3.1 Wavelength chaos

The first variable to be considered for chaotic carrier cryptographic purposes is the wavelength of a tunable laser [37, 58]. The experimental setup of this system is presented in Figure 18.

The chaotic oscillator is constituted by

- a Distributed Bragg Reflector (DBR) laser diode tunable around 1550nm by the current from a second electrode. This component is noted "DL" in the figure,
- a component with a non-linear relationshop between the wavelength and optical power variables: this element performs as an optical spectral filter and is constituted by a birefringent crystal ("NL" in the figure) placed between two cross polarizer

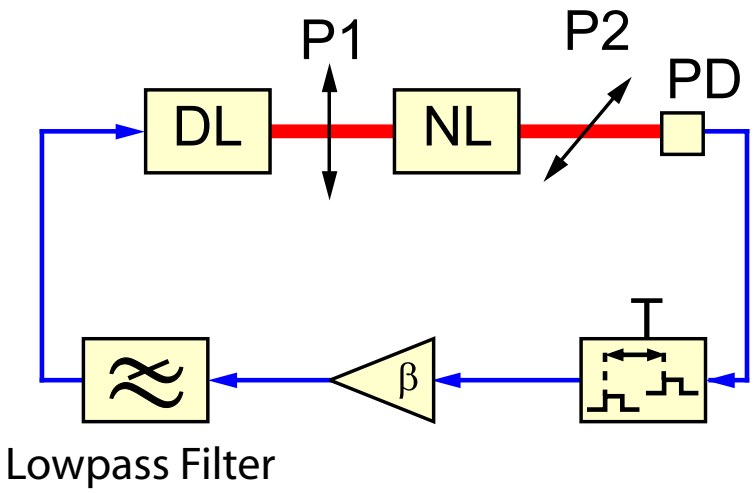


Figure 18: Experimental setup of the wavelength chaos generator.

plates (P1 and P2),

- a photodetector ("PD" in the figure),
- a delay line T,
- a gain β,
- and a first-order low pass filter ($f_c = 20kHz$) that determines the response time of the feedback loop.

The chaotic oscillations of this system are modeled by an Ikeda differential equation:

$$x(t) + \tau \frac{dx}{dt}(t) = \beta \cdot F_{NL}[x(t-T)] = \beta \sin^2[x(t-T) + \phi], \tag{19}$$

where $x(t)$ represents the normalized chaotic signal (proportional to the physical dynamic variable of wavelength deviation) and $F_{NL}[.]$ is the non-linear function.

The experimental bandwidth of this system is roughly 20 kHz [58], is limited by the tunability speed of the laser diode, and is not sufficient to encrypt signals at optical telecom frequencies.

2.3.3.2 Coherence modulation chaos

The use of coherence modulation is a physical trick that adds an additional security level [59, 60]. The absence of variation of the intensity of the transmitted signal constitutes a level of encryption on top of the encryption generated by the chaotic variation of the carrier coherence.

A broadband optical source, in this case a super luminescent laser diode, feeds an unbalanced Mach-Zehnder interferometer whose optical path difference (OPD) D_1 is greater than the coherence length L_c of the optical source. This unbalanced interferometer duplicates the incoming wave trains into twin wave trains separated by a distance D_1. Since D_1 is much greater than L_c, there are no interferences between the wave trains at the output of the interferometer. Thus, there are no detectable variations of the light intensity when the optical signal is modulated by the electrical voltage $V(t)$. During an electro-optic modulation, the information is encoded by the distance between two wave trains. The dynamical model for this setup is very similar to the wavelength chaos one: only the non-linear function differs. This non-linear function is performed by a second unbalanced Mach-Zehnder modulator that duplicates the two wave trains. At the output of this modulator, we can observe modulated interferences from the electro-optic effect of the first modulator. These interferences can be obtained only if the second modulator's static imbalance is the same as the first one's. A photodiode detects these interferences. The electrical signal output from the photodiode is then delayed, amplified, and fed back to the electrode of the first modulator. The experimental setup of this coherence modulation emitter is described in Figure 19.

This system presents an increased level of security but has limited bandwidth (10 kHz [59, 60]), which severely restricts any application of this system to optical networks.

2.3.3.3 Phase chaos

We have seen how wavelength chaos and coherence modulation chaos do not meet the requirements for a real-time crypto-system for optical networks. Another variable was

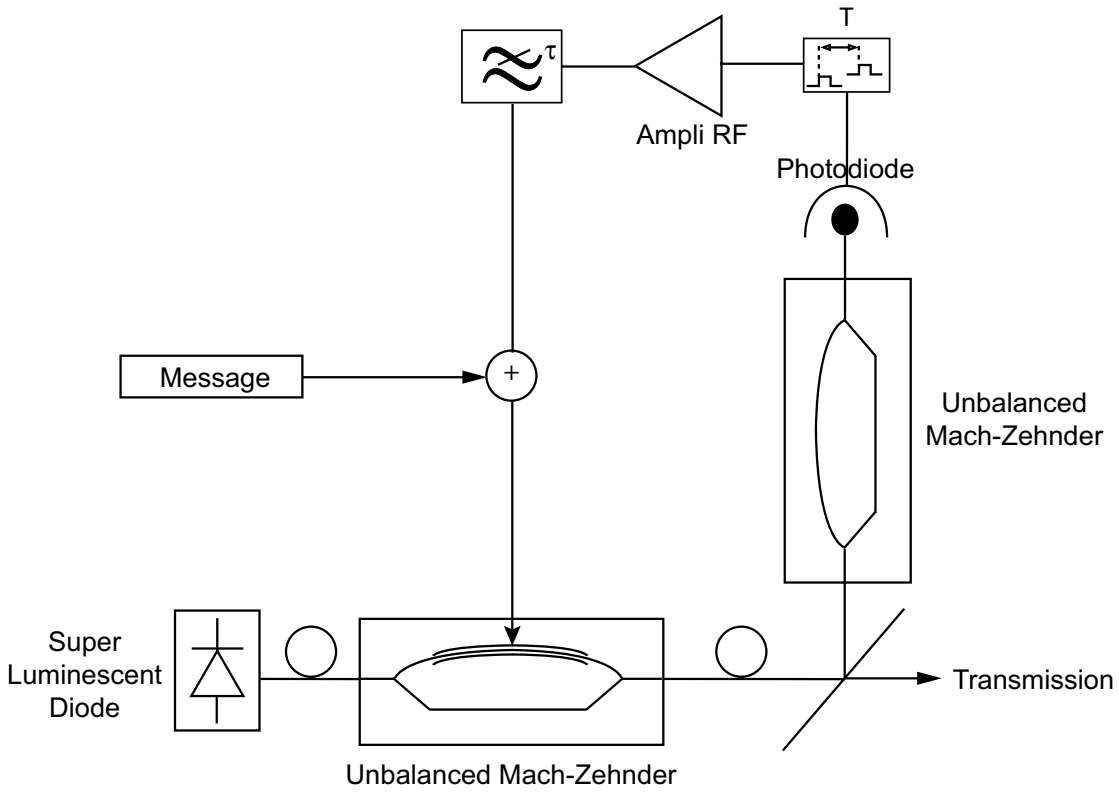


Figure 19: Experimental setup of coherence modulation chaos.

therefore used in an attempt to achieve a wideband chaotic dynamic: optical phase. The objective was to generate broadband chaotic oscillations of the optical phase.

The emitter of a crypto-communication based on the optical phase is presented in Figure 20. A phase modulator receives light from an ultra-stable laser source emitting at 1550 nm. The output of the modulator goes through a 2x2 optical coupler before being detected, amplified, filtered, and fed back on the modulation electrode of the modulator. Two branches of the optical coupler are connected together and effectively form an optical cavity of delay T. This coupler also realizes the non-linear function: the output of the coupler is non-linearly linked to the input by an interference process as long as the phase modulation is faster then the optical cavity delay.

Only the emitter was developed experimentally. A very wide bandwidth was obtained: it stretched from tens of kHz to roughly 5 GHz [36]. Unfortunately, the application of such

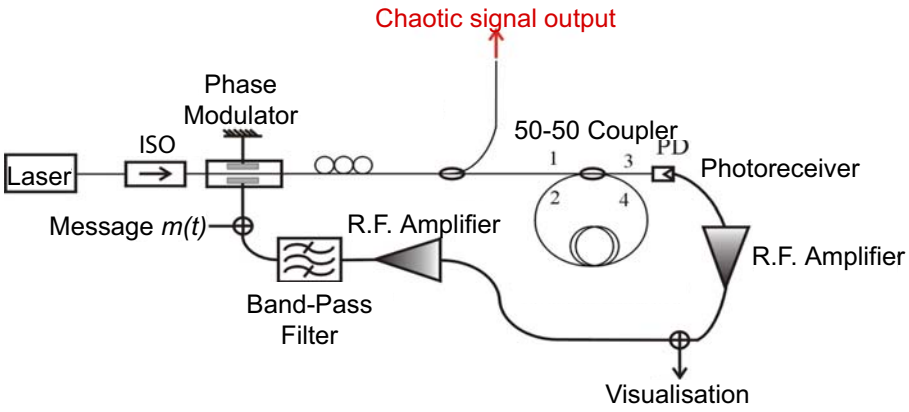


Figure 20: Experimental phase chaos generation setup.

a system to optical networks is limited by the optical cavity stability problems.

2.3.3.4 Intensity chaos

The initial research on intensity chaos cryptography (P. Lévy's thesis [62]) constitutes the basis the work of this dissertation. The variable that fluctuates chaotically is now the optical intensity. The experimental setup is shown in Figure 21.

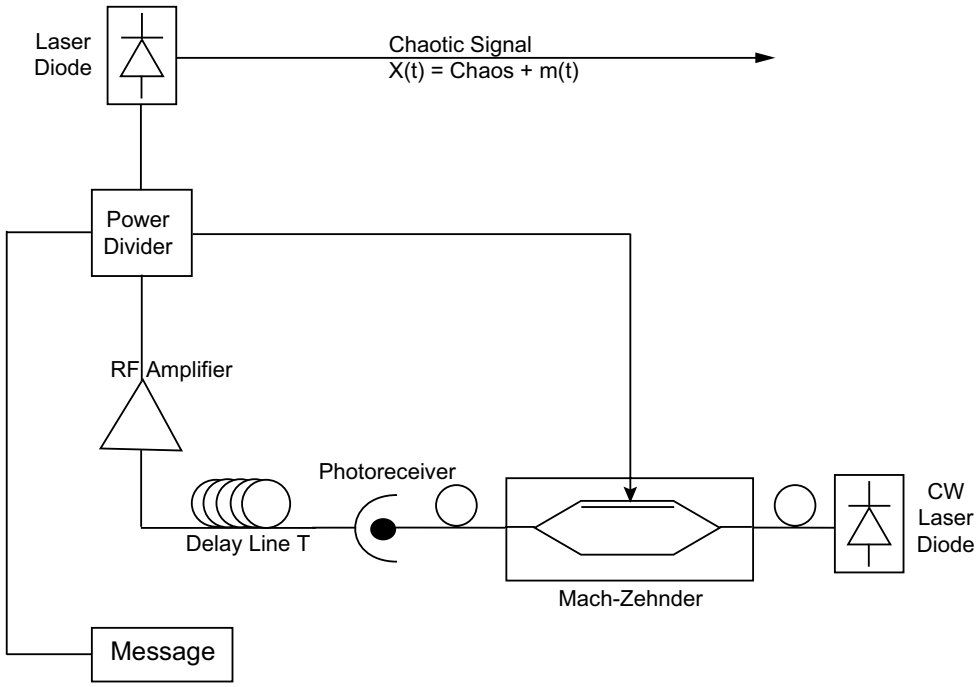


Figure 21: Experimental intensity chaos generation setup.

The emitter is built around an electro-optic Mach-Zehnder interferometer (MZI) illuminated by a continuous wave laser diode. The MZI output is fed back through a delay line, a photoreceiver, and an RF amplifier to the modulation input of the MZI. A part of this signal is used for transmission purposes. With the components available at the time of this research, the bandwidth of the generated chaos corresponds to the interval $25 - 150$ MHz [41].

The present research is in the continuity of this initial work with the objective of increasing the bandwidth of the system to make it suitable for multi-Gigabit networks.

2.3.3.5 Comparing results to date

We have seen the various opto-electronic feedback system approaches to chaos cryptography. Each is an attempt to provide a method for encrypted optical networks. Table 1 summarizes the performance of each system for three important telecom characteristics.

The first line compares the bandwidth of each system. The bandwidth is a measure of the maximum throughput. The second line is the system flexibility and gives an idea of the conditions under which the systems will be operational outside of the controlled environment of a laboratory. Finally, the cost of each system is compared.

Table 1: Comparative table for different chaotic variables.

	Wavelength	Coherence	Phase	Intensity
Bandwidth	150MHz	200MHz	>10GHz	>10GHz
Flexibility	High	High	Medium	High
Cost	High	High	High	Low

The bandwidth line clearly separates the systems; there are those that can reach multiple GHz and those that cannot. For example, the bandwidth of the wavelength chaos system is limited by the tunability speed of the laser diode. For this field, phase chaos and intensity chaos present the best results. The system flexibility, on the other hand, highlights a disadvantage for the phase chaos, which necessitates very high stability of the optical loop. Non-negligible for a telecom application, the relatively low cost of the intensity

chaos setup is a clear advantage. Intensity chaos provides the only setup implemented with off-the-shelf optical, electronic, or opto-electronic components. On the other end of the cost spectrum, the wavelength tunable laser diode for the wavelength chaos is expensive, as are the unbalanced Mach-Zehnder interferometer and the superluminescent laser diode for the coherence modulation chaos. For phase chaos, the high price is caused by the highly stable laser diode.

The combination of these factors clearly points to the intensity chaos as the most promising research avenue for high-speed chaos cryptography at a relatively low cost.

2.3.4 OCCULT Contract

The GTL-CNRS Télécom laboratory is one of the participants in the OCCULT (Optical Chaos Communication Using Laser Transmitters) contract. This contract, IST-2000-296683, is administered by the directorate of the General Information Society of the European Commission. This contract brought together many European laboratories competent in the fields of optical networking and chaos. Our partners are

- Universitat de Les Illes Balears,
- University of Wales,
- Technische Universität Darmstadt,
- National and Kapodistrian University of Athens,
- Universita Degli Studi di Pavia,
- Opto Speed SA,
- Consejo Superior de Investigaciones Cientificas.

The OCCULT contract text specifies a certain number of objectives to reach. These objectives are both experimental and theoretical on topics such as speed, security, and

transmission length. Without detailing each deliverable or milestone specified in the contract text, the progression toward a secure communication system is done following five workpackages. The first element consists of the realization and the study of the chaotic emitter. The second explores the synchronization capabilities of the receiver. A synchronized receiver sets the stage for the third element: the study of the communication link in back-to-back configuration. The fourth element studies the evolution of this communication quality as a function of distance. The fifth element is solely numerical simulations of the overall system.

While all of the contract objectives do not fall within our purview, they do lead to the end-to-end characterization of a chaos cryptography communication system. This thesis work runs on a parallel track to the OCCULT contract objectives.

Conclusion

This first chapter was an initial approach to the chaotic behavior, through the study of various remarkable non-linear dynamical systems. The properties of chaotic systems were illustrated in continuous time by the harmonic pendulum and in discrete time by the logistic map application. By modifying a control parameter, we have observed the evolution of the logistic map behavior, from stable fixed point to single and multi-period oscillations, all the way to chaotic behavior. Each fundamental characteristic of chaotic dynamics was then presented: determinism, sensitivity to initial conditions, pseudo-randomness.

We presented analysis tools that apply specially to chaotic dynamics (phase space representation, spectrum plots, autocorrelation and bifurcation diagram). These tools were illustrated with Chua's circuits, which generate simple chaotic dynamics, allowing for the quantification of certain aspects.

Chua's circuits evidence a remarkable property of chaotic systems: synchronization. Two non-linear dynamics generated by separate systems can synchronize and oscillate in an identical fashion, the receiver system duplicating the emitter oscillations. By widening

our view of these properties to the scope of optical communication, we naturally come to the objective of this research: develop a cryptography application using a chaotic carrier wave. This work is more specifically applicable to securing high bit rate optical networks.

Various examples of chaos generators developed for chaos cryptography purposes were then detailed. These examples illustrate the current techniques implementing the encryption directly at the physical layer of the optical network. These systems have been classified based on the technique used for the generation of the chaotic dynamic: we made the distinction between all optical systems and opto-electronic ones. We presented systems using injection lasers, external cavity lasers, and opto-electronic systems with different dynamical variables (wavelength, optical phase, intensity...).

Our work is an extension of the research of Pascal Lévy [62]. That research developed a complete opto-electronic encryption system using optical intensity as its chaotic observable. However, the frequency range of this system was limited (<150 MHz). We have extended the principles of this first system and the bandwidth covered to fulfill our goal of secure communication at multi-Gbits/s.

The next chapter develops the operating principles and the characteristics at the heart of our system: the electro-optic non-linear delay oscillator. The third chapter provides a global study of the communication system, both in terms of performance and encryption. The fourth chapter presents the limitations of the system we noted during our experimental work and proposes improvements. The fifth chapter looks at the message signal and explores various message formats.

CHAPTER 3

CHAOS GENERATION AND MESSAGE INSERTION

In the previous chapter, we explored the context and positioning of this research within the field, specifically with reference to the framework of the OCCULT contract.We have also evoked the progression of this research axis in the P.-M. Duffieux optical laboratory (Section 2.3.3).

The performance objectives are clear, quantitatively and qualitatively: to encrypt, transmit and decrypt with acceptable quality an optical message at bit rates compatible with modern optical communication networks.

In order to accomplish these tasks, we will first study chaos generation for the particular type of system we are using, to determine the optimal conditions for the implementation of the chaotic emitter. We can then characterize the experimental emitter of our system.

3.1 Operating principle

The global system termed "emitter" can be separated into two parts. The first part is the realization of a non-linear oscillator tuned to behave chaotically. We study the operating principle of this oscillator in Section 3.1.1.

The second part deals with the insertion of a message into the chaos generator. For a communication system, the message transmission is the principle objective. We will detail several fundamentally different methods of encoding the message into the chaotic transmission in section 3.1.2.

3.1.1 Chaos generation

The non-linear oscillator we are implementing must behave chaotically in some regions of its parameter space. The general principal that we have selected is based on a system that was originally studied by Ikeda [46–48] and is part of the particular family of non-linear delay dynamical systems. These systems exhibit interesting properties because of the

presence of a large delay in the feedback loop. The delay increases the degree of liberty of the dynamical solutions and leads to an infinite dimensional phase space. In general, delay dynamical systems present complex dynamics of high dimensions and are very interesting for our purpose since the complexity of the generated chaos heightens the security of the encryption.

The experimental system studied by Ikeda corresponds to a ring cavity, called the Ikeda ring cavity (Figure 22), inside which a two-level absorber is inserted. This absorber dephases and attenuates the electric field propagating through the absorber as a function of input intensity.

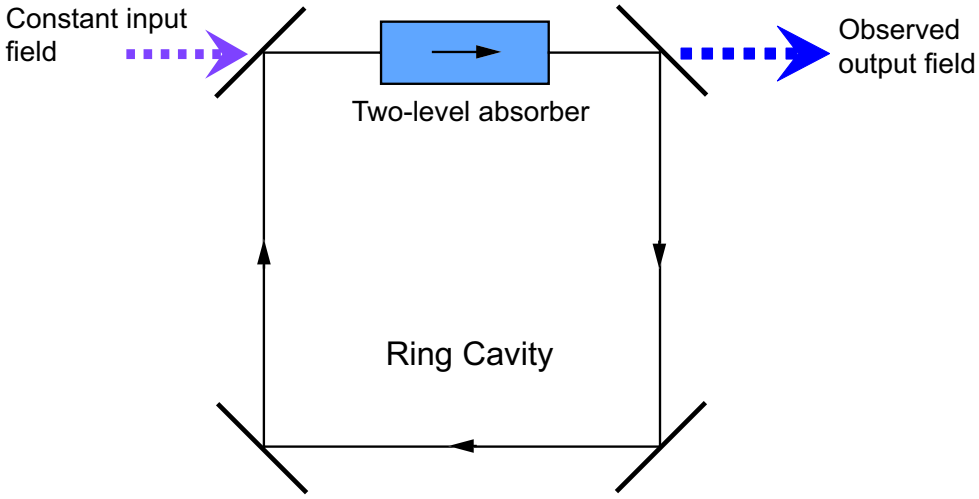


Figure 22: Experimental Ikeda setup.

The effect of the absorber on the observed output electric field is characterized by integrating the Maxwell-Bloch equations over the length of the absorbing cell (20):

$$\frac{\partial E}{\partial z} = 4\pi i N \mu k \rho, \tag{20a}$$

$$\frac{\partial \rho}{\partial t_R} = (i\Delta\omega - \gamma_\perp)\rho - i\mu w E, \tag{20b}$$

$$\frac{\partial w}{\partial t_R} = -\gamma_\parallel (w + 1/z) + i\mu (\rho^* E - \rho E^*)/z, \tag{20c}$$

where $t_R \equiv t - z/c$ is the delay term, ρ and w are, respectively, the dimensionless polarization and population inversion of the two-level atom; μ is the transition moment dipole and

$\Delta\omega \equiv \omega - \Omega$ is the detuning frequency between the input wave frequency ω, the dipole transition frequency Ω, k is the wave number of the electric field in vacuum, $\gamma_\perp$ and $\gamma_\parallel$ are the transverse and longitudinal relaxation rates and N is the density of the atoms [48]. After some manipulations and approximations, Equation (20) can be cast under the form primarily studied by Ikeda:

$$\frac{dx(t)}{dt} = -x(t) + \pi\mu\,[1 + 2B\cos(x - T - x_0)] \tag{21}$$

where μ is the bifurcation parameter proportional to the optical intensity at the input of the ring cavity and $B(< 1)$ represents the dissipation of the electromagnetic field in the cavity. The system time constant was normalized to 1 in equation (21) [47]. An Ikeda-type system can also be expressed by two equations, one of which is specific to the non-linearity of the system. Equation (21) can then be divided into two equations:

$$\frac{dx(t)}{dt} = -x(t) + F_{NL}(x(t - T); \mu), \tag{22a}$$

$$F_{NL}(x; \mu) = \pi\mu[1 + 2B\,\cos(x - x_0)], \tag{22b}$$

where Equation (22a) describes the general form of the non-linear delay dynamical system, and Equation (22b) is specific to the non-linear device implemented in the Ikeda system. By adopting a functional block approach, we can say the Ikeda system is composed of three blocks: the first one corresponds to the delay, the second one to the system gain, and the third one to the non-linearity. A fourth block, not present in the model, but an integral part of any physical system, is the filtering with at least a low pass component.

The Ikeda system behavior exhibits successive bifurcations [47] and, under certain conditions, chaotic behavior [48]. This study validates the chaos generation model consisting of non-linear, gain, and delay elements. These works have sparked the research on optical chaotic dynamics in the laboratory P.-M. Duffieux [57].

The model that we base our research on is greatly inspired by the Ikeda scheme. The three functional blocks are kept (non-linearity, gain, and delay). The main difference is with

the filtering function. The initial model included a low-pass filter. Since we are attempting to reach frequencies on the order of 10 GHz, consideration of only a simple low-pass filter is not realistic. The wide-band components also filter continuous signals, and even the lower frequencies, typically up to 30 kHz. In order to match modern techniques, our model includes a band-pass filter.

Experimentally, the system implemented to generate chaotic dynamics is based on the diagram of Figure 23. The non-linear function is necessary to obtain chaotic dynamics. Sweeping one extrema of the non-linear function is mandatory for the system to behave in a chaotic manner, and the number of swept extrema controls directly the complexity of the generated chaotic dynamics. We are therefore looking to sweep the greatest possible number of extrema to obtain high complexity dynamics. The linear gain element, by amplifying the input signal to the non-linear function, is responsible for the sweep of multiple extrema, which makes our system more non-linear and increases the complexity of the generated dynamics. The output of the "gain non-linearity" combination is then delayed before being fed back. This delay increases the degree of freedom of the solutions corresponding to the dimension of the phase space.

Without proceeding directly to the experimental implementation details of this principle diagram (Figure 23), let us consider the variable $x(t)$ as the input of the non-linear function. After the non-linearity and the delay, we observe the signal $F_{NL}[x(t-T)]$. If $h(t)$ is the impulse response of the linear feedback (filter function and gain), we can express $x(t)$ as convolution:

$$x(t) = \beta \{h(\theta) * F_{NL}[x(\theta - T)]\}(t) = \beta \{h * c\}(t), \tag{23}$$

where β represents the gain of the chaotic oscillator and $c(t)$ the chaos at the output of the oscillator.

This method of modeling the system, which stems directly from the block representation of Figure 23, is an integral type formulation and leads to Equation (23) with the convolution of two signals in the time domain. Equation (23) is the general, intrinsic, form

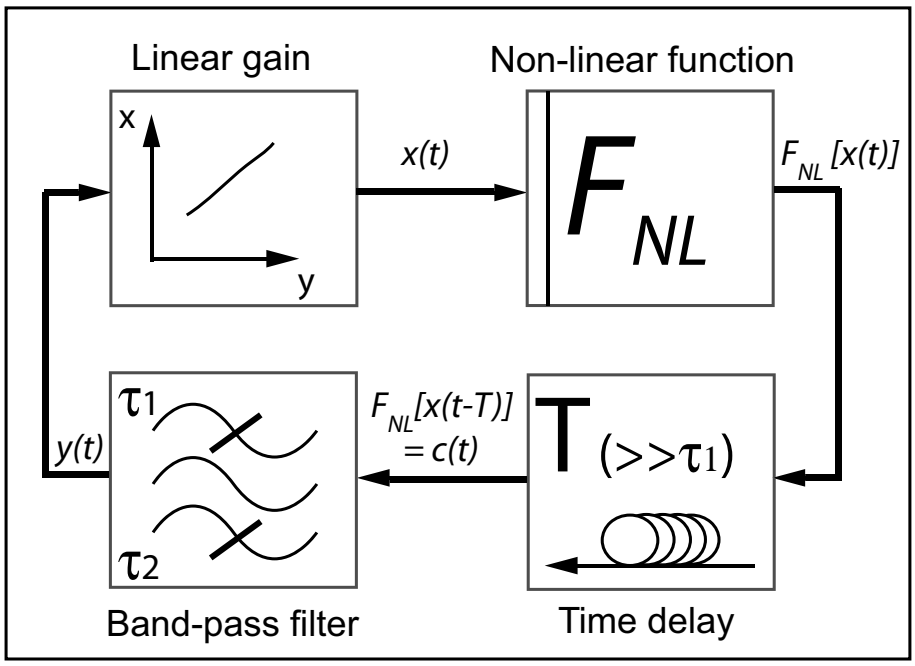


Figure 23: Principal diagram of the implemented chaos generator.

of the system described by Figure 23 and relies on the hypothesis of separability of the functions described previously (delay, gain, linear dynamic process, non-linear adiabatic transformation). By taking into account the characteristics of each component, we will obtain Equation (29).

Since the emitter is capable of producing chaotic dynamics under certain conditions, we need now to incorporate the message into the transmission in order to fulfill the second function of the emitter.

3.1.2 Message insertion techniques

In a cryptographic system, the objective is to transmit a message securely from emitter to receiver. The message signal can take on two forms, analog or digital. Multiple techniques exist to encode the message onto the chaotic carrier. Some have been specifically developed for digital signals, others can also encode analog signals.

Before proceeding, we must distinguish the difference in meaning between "coding" and "encoding". Since the typical process comprising of the transformation of a digital

message and its analog integration in the emitter system is of only one step, the two terms (coding and encoding) are often used interchangeably. Although of close etymology, those two terms have fundamentally different meanings within the context of this dissertation. The coding of the information deals with the algorithms that transform a numerical message into a series of analog symbols of advantageous properties for transmission. For example, morse code transforms each letter of the alphabet into a sequence of long and short sounds. More closely related to our present work, the coding schemes Return to Zero (RZ) and Non Return to Zero (NRZ) are widely employed. There are many other information coding formats [63,100]. On the other hand, the term "encoding" refers to the method the message, properly coded, is incorporated into the chaotic signal to form the signal to be transmitted to the receiver. Since the communication method we use presents these two different steps, a terminology clarification was of necessary.

The limitations of our testing equipment impose NRZ message coding. The message that we use is, therefore, a pseudo-random bit sequence (PRBS) with NRZ coding. Since the coding is set by the testing equipment, we concentrate on the encoding aspect in the first four chapters. Chapter 6 will focus explicitly on coding and message modulation formats. The encoding of a message on a chaotic carrier wave poses interesting problems.

For chaotic communication, three classic encoding schemes exist: chaos masking, chaos shift keying (CSK), and chaos modulation. Each encoding method has advantages, disadvantages, and constraints relative to the cryptographic quality of the system.

3.1.2.1 Chaos masking

The simplest case is chaos masking. Here, the message is added to the chaotic signal generated by the oscillator, then transmitted to the receiver (Figure 24).

The variations of the message amplitude are hidden by the chaotic fluctuations of the carrier signal intensity. The masking technique requires two conditions: the first one is that the spectrum of the message needs to be completely overlapped by the spectrum of the generated chaos. If not, a simple filtering operation can provide at least some information

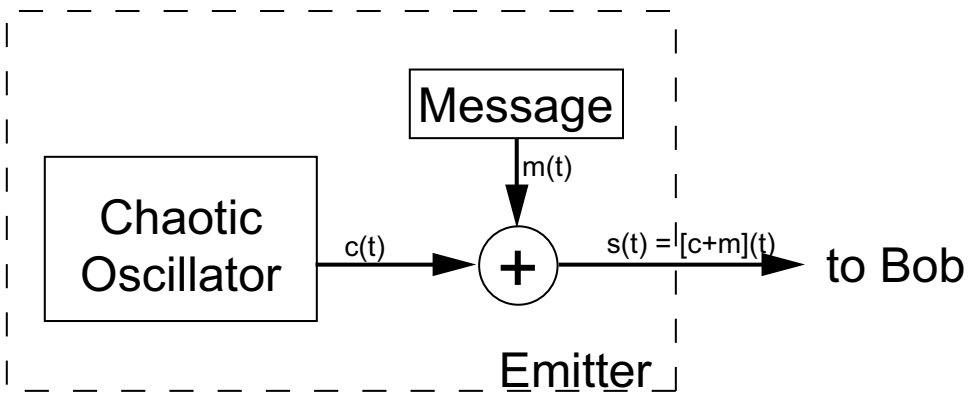


Figure 24: Chaos masking.

on the message to an eavesdropper. The second condition relates to the efficiency of the masking. The message amplitude, $m(t)$, must be sufficiently small relative to the chaotic fluctuations $c(t)$ of the chaotic carrier. An empirical approach gives that this condition is verified for $m(t) \lessapprox 0.1\, c(t)$. The message is now of a size comparable to that occupied by the noise on the transmission channel. Message and noise are then intermingled. Significant noise levels reduce the communication quality very rapidly. Consequently, this type of encoding is seldom used for communication because of the noise problem.

3.1.2.2 Chaos shift keying

Another encoding format, chaos shift keying (CSK), was developed exclusively for binary messages. We can distinguish two forms of CSK: coherent CSK and non-coherent CSK [20]. The CSK principle is to change the dynamics of the chaotic oscillator as a function of the binary message that is being transmitted. The receiver is set to synchronize properly on one of the two emitter dynamics. Switching between the two emitter dynamics generates an important error at the receiver. The receiver is capable of detecting the changes in the emitter dynamics by analyzing the error message and can, therefore, extract the message from the transmission.

Non-coherent CSK was studied in our laboratory on an Ikeda system where the chaotic variable was the optical wavelength of the carrier wave. A total of six experimental parameters are adjustable in the experimental setup [20]: the non-linear function F_{NL}, the system

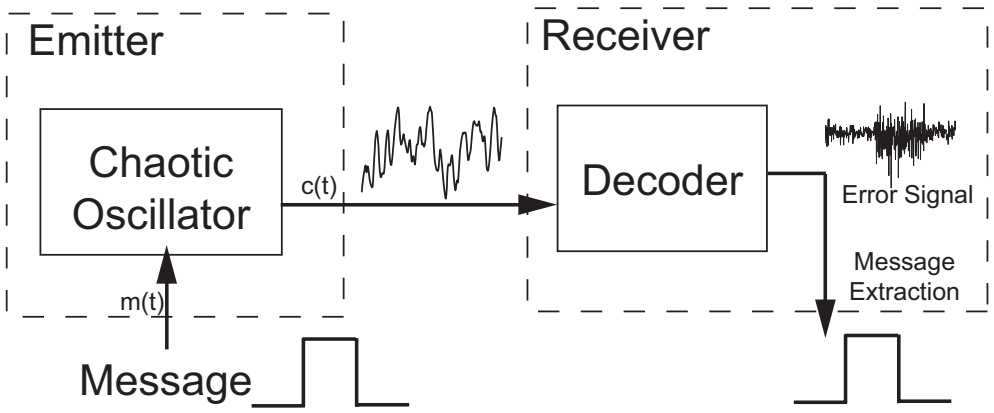


Figure 25: Non-coherent CSK: principle.

gain β_λ, an induced phase parameter ϕ, the filtering constants τ and θ, and the delay T of the system. Equation (19) models such a system with $x(t)$ representing the emitter wavelength. To decode and extract the message from the transmitted signal, the receiver parameters are tuned, in the absence of a message, to minimize the error signal. The detuning resulting from a system parameter modulation translates to an increase in the error message. The analysis of the variations of the error message amplitude decodes the message (Figure 25).

An eavesdropper tapping the transmission line should not be able to detect the variations of the emitter dynamics, whereas the authorized receiver will base his decoding on these changes. This requirement limits the parameters used to implement CSK. Furthermore, from an experimental standpoint, modulating the parameters F_{NL}, τ, θ and ϕ of Equation (19) is impractical. The only two accessible parameters are the system gain β_λ and the delay T (see Figure 18). Modulating the parameter β_λ does not allow for proper message extraction without introducing easily detectable variations of the dynamics on the transmission line. Therefore, the study focused mostly on implementing T as the modulated parameter. The results were satisfactory in terms of security and communication quality [19]. The principal limitation of these systems is the encoding speed. The system components need to withstand modulation at the message bit rate. Another upper bound on the communication speed is the time the receiver needs to synchronize on the new emitter dynamics after each bit.

Coherent CSK is based on the same principal [87]: detection of emitter dynamics changes by the receiver. In the case of coherent CSK, the switching is done between two separate circuits oscillating chaotically with two different attractors. The limitations due to loss of synchronization and resynchronization time remain the same.

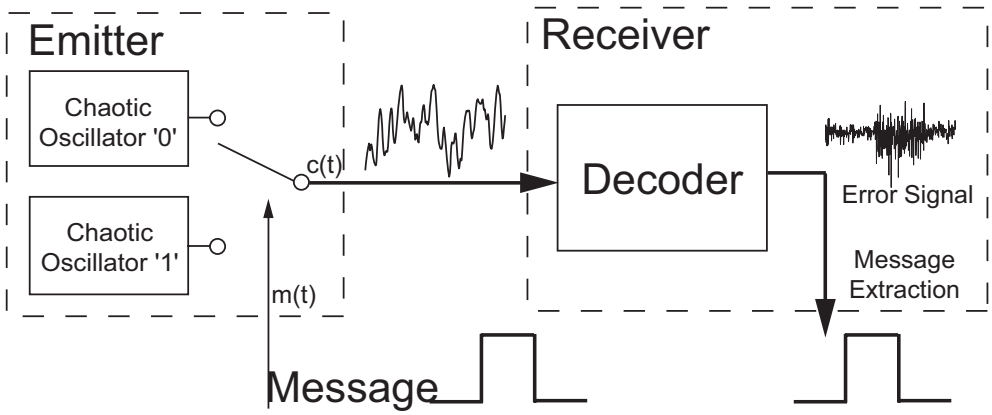


Figure 26: Coherent CSK: principle.

3.1.2.3 Chaos modulation

There is a third message encoding scheme: chaos modulation. In this case, the message is incorporated directly into the chaos oscillation feedback loop. The emitter chaotic dynamics are modified by the message. This cryptographic technique has been implemented multiple times in our laboratory [20, 41, 57, 58].

The message $m(t)$ can be inserted into the emitter by addition after the delay function (Figure 27). For an optical power P_0 of the chaotic oscillation at the point where the message is inserted, we set the peak optical power of the binary message as αP_0. The parameter α represents the masking efficiency with respect to the chaotic carrier.

Equation (23) of the chaotic oscillator can be modified to take the message into account. As explained above, the message is inserted by addition in between the gain and the filter elements. Therefore, the term $F_{NL}[x(\theta_t - T)]$ which is convolved with the $h(t)$ transfer function becomes $F_{NL}[x(\theta_t - T)] + \alpha m(\theta_t)$. Therefore, Equation (23) becomes:

$$x(t) = \beta \{h(\theta_t) * [F_{NL}[x(\theta_t - T)] + \alpha\, m(\theta_t)]\}(t) = \beta \{h * c\}(t) \tag{24}$$

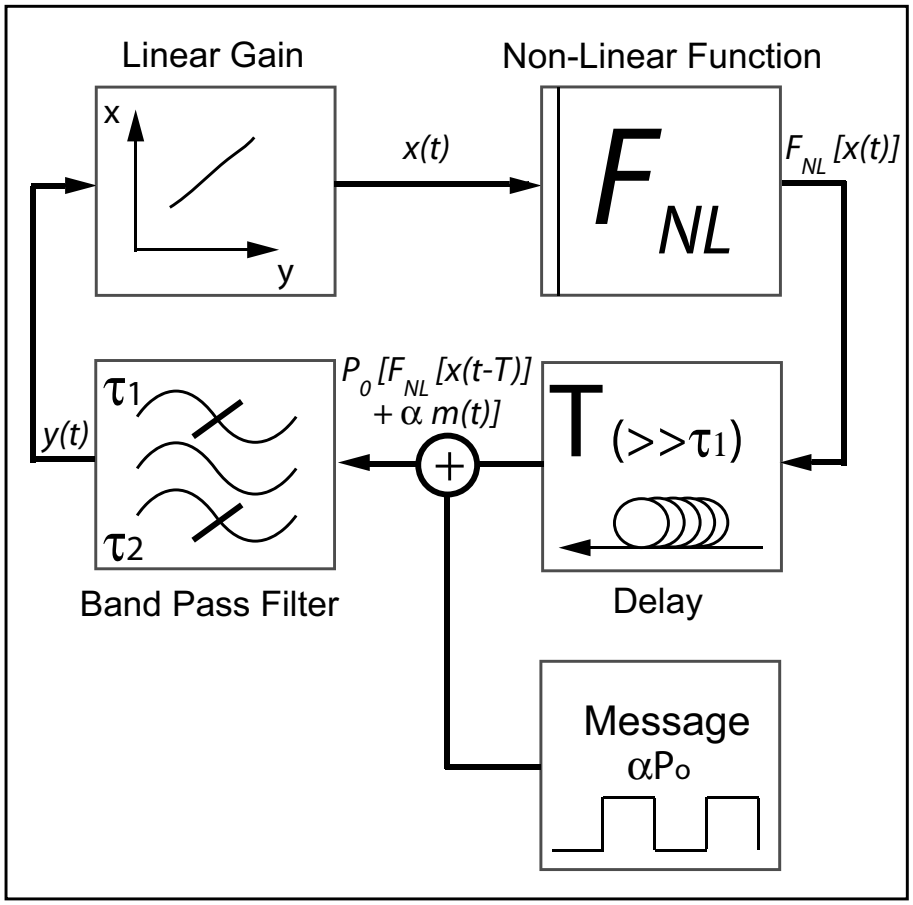


Figure 27: Chaos modulation: principle.

An important advantage of this encoding scheme is that synchronization is not lost with each message bit. Therefore, the resynchronization time is not a limiting factor, contrary to CSK encoding. We can therefore reach high bit rates, limited only by the bandwidth of the chaotic dynamics and not by the resynchronization time. The system limitations, in terms of security and speed, will then be dependent on the α factor from Equation (24), quantifying the masking of the message in the transmission line, and on the system bandwidth. The term "masking" may be confusing since we are dealing with chaos modulation and not chaos masking. Still, the message amplitude still is relevant: the pattern of the message should not be visible in the transmitted signal. The generated chaos still acts as a masking agent for the message, even when the message is part of the chaos generation process.

For our chaos cryptography experimental implementation, we selected this the encoding scheme, as much for ease of implementation as for the system's high speed potential.

3.2 Experimental setup

The experimental setup consists of the implementation of the principal diagram (Figure 27). We made use of the experience accumulated during the doctoral work of Pascal Levy [62] to avoid certain problems that arose in the past, specially with high power losses in the feedback loop.

Firstly, we will motivate the specific component choice. Secondly, we will justify the experimental layout of the emitter. Finally, the characteristics of the system will be successively presented and analyzed.

3.2.1 Component description

The implementation of the block diagram requires the following components: a telecom monomode laser diode, a photoreceiver, a wideband RF amplifier, a Mach-Zehnder electro-optic modulator, and a delay line. The specifics of the insertion of the message into the chaos feedback loop will be detailed later.

3.2.1.1 Laser diode

The Distributed FeedBack (DFB) laser diode continuously emits light. The model we selected is the 1905 LMI from Alcatel. This pigtailed laser diode illuminates the electo-optic modulator, described later on in this manuscript. The DFB type of laser presents high selectivity and high wavelength stability, making the laser highly monomode, which is important for optical WDM telecom applications. The specific laser diode at the emitter emits at 1550.06 nm, corresponding to the ITU channel centered around the WDM frequency of 193.3 THz.

A DFB laser resembles a classic Fabry-Pérot laser. The particularity of the DFB design is that the Bragg grating is distributed over the length of the laser cavity. This structure is illustrated in Figure 28. The grating produces the same effect as a fiber Bragg grating,

reflecting a single wavelength while letting the other pass. With this system, a DFB laser emits at a high specific wavelength. This type of laser gets its name from the continuous distribution of the Bragg grating over the length of the laser cavity [2].

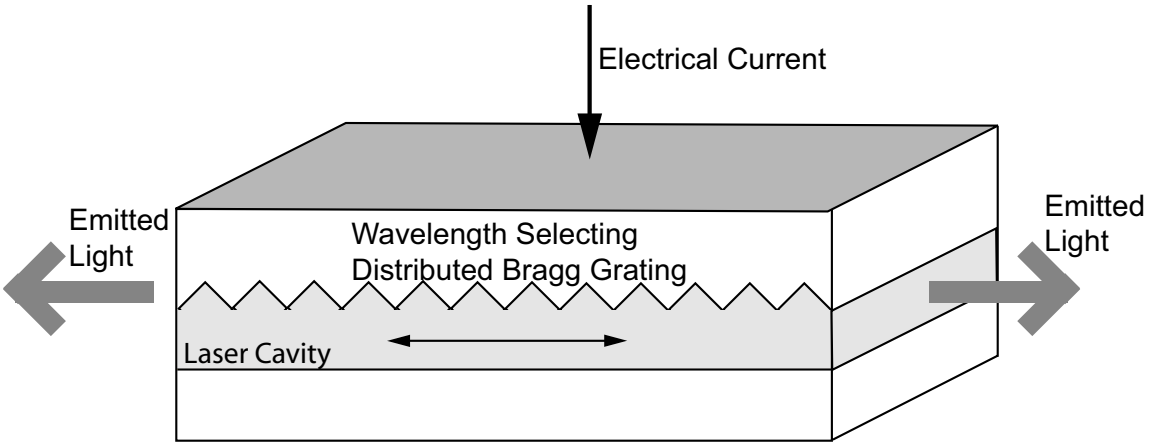


Figure 28: Structure of a DFB laser diode.

The output optical power of the laser is a function of the diode injection current. The threshold current is 15 mA and the P-I characteristic of the laser diode has a slope of 153 mW/A. Constant output optical power is achieved through proper control of the diode injection current. Similarly, a stabilized output wavelength is achieved through proper temperature control.

The DFB laser serves as the energy source for the electro-optic non-linear oscillator but does not intervene in the dynamical process (unlike the external cavity lasers).

3.2.1.2 Photoreceiver

The second element of the linear gain chain converts the received light into electrical tension. We have chosen for this task a Miteq photoreceiver with a band pass region stretching from 30 kHz up to 12 GHz, as illustrated on Figure 29. This figure was reproduced from the manufacturer's specification sheet as we did not have the necessary equipment.

This photoreceiver comprises two parts: a photodiode and a trans-impedance amplification stage. The photodiode converts the input light into electrical current with a response

of 0.9 A/W at λ = 1550 nm. This current then flows through a amplifier with a typical trans-impedance gain of 2240 Ω. With this combination of photodiode and amplifier, the opto-electronic conversion factor is 2 V/mW$_{optical}$. Another important characteristic of these photoreceivers, which greatly influenced our choice, is their maximum output voltage of 4 V. We need to keep in mind that the objective of the gain stage is to amplify as much as possible the signal inside the feedback loop in order to drive the electro-optic modulator with a significant signal amplitude. Since the gain needs to remain linear, the maximum optical power at the input of the photoreceiver should be 2 mW. The photoreceiver output signal is then amplified by the third element of the linear gain: the wideband RF amplifier.

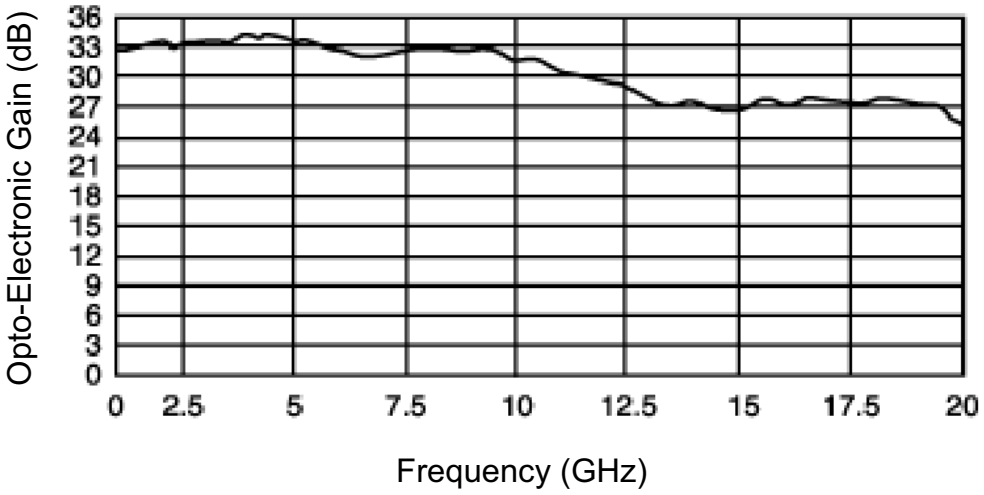


Figure 29: Typical opto-electronic gain of Miteq photoreceivers.

3.2.1.3 Radio frequency amplifier

The RF amplifier, also termed modulator driver or just driver, is connected to the modulation electrode and drives the electrode voltage. The objective is for the electrode voltage to span multiple $V_{\pi,RF}$[1] to sweep multiple extrema of the non-linear function; hence, the importance of the maximum output voltage of the amplifier. Obviously, the bandwidth of the amplifier must be as wide as possible.

[1] Roughly 4.2 V for our modulators, defined in the next section

The RF amplifier we selected is the 100CP broadband amplifier from German manufacturer SHF Communication Technologies AG. The driver bandwidth reaches from 30 kHz all the way to 25 GHz for a typical gain of 18 dB. The maximum output power is 26 dBm, which on a 50 Ω line corresponds to a voltage of 12 V. We are therefore very close to sweeping three extrema of the non-linear function. Figure 30 plots the S_{21} transmission parameter as a function of frequency for the two amplifiers we used. A catalog option that was of particular interest to us was the ability to order a matched pair of amplifiers. The characteristics of the amplifiers are then certified to be no farther apart than 0.5 dB over the bandpass frequency range.

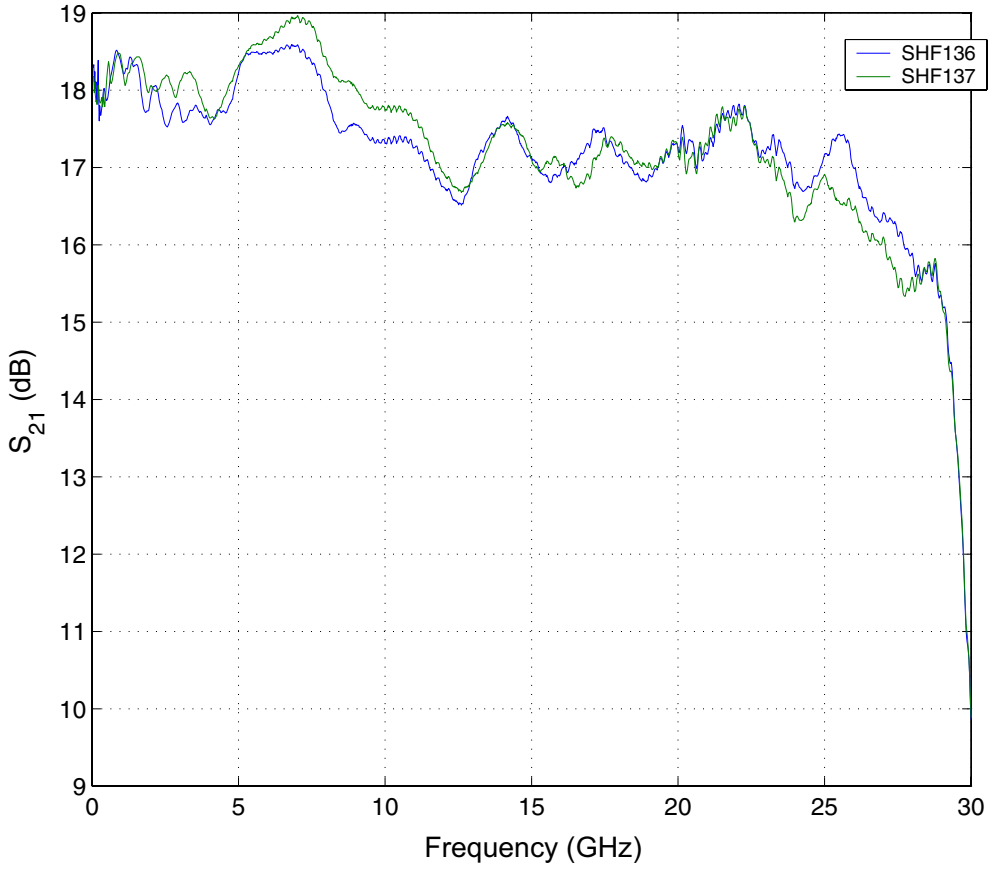


Figure 30: SHF RF amplifier transmission coefficients.

3.2.1.4 Modulator

The electro-optic modulator is the central component of the system without which no chaotic dynamics can be achieved. Indeed, the modulator realizes a non-linear function through its RF voltage controllable accordable interference function. Selection of the modulator required particular care. The products of EOspace, a company based in Redmond, WA, were retained for our system because of their performance in terms of bandwidth, low half-wave voltage and low insertion losses. The functioning of a modulator and the characteristic values that define the modulator and its qualities are now explained.

The intensity electro-optic modulator is a Mach-Zehnder interferometer. The input optical beam is separated in two, each beam propagating in two different branches. The difference in optical path length of each branch creates a phase difference between the two signals. This difference translates into interference when the two signals are recombined. The interferometer becomes an electro-optic modulator when the optical path length difference is controlled, i.e. modulated, by an external electrical signal [102].

The modulation quality of the component rests on the control of the modulated branch optical path length. Lithium Niobate ($LiNbO_3$) is a material with important electro-optic properties. An electric field changes its index. Since optical path length is the product of distance by propagation medium index, any change in the medium index modifies, for a fixed distance, the optical path length. Therefore, the electrical signal $V(t) + V_b$ applied to the modulation electrode (Figure 31) creates an electric field and modifies the optical path length of the modulated branch. The signal $V(t)$ is the dynamic part of the modulation signal, while V_b is a fixed bias voltage that sets the modulator operating point. Light propagating in the branch is, therefore, modulated by this electric signal.

The crystalline structure of $LiNbO_3$ presents two planar symmetries (X and Y planes). The material presents different properties along each axis. The electro-optic effect of the crystal impose a polarization along the Z axis for maximum effect. Thus, a Z-cut or an X-cut can be used for the material. Z-cut modulators present lower half-wave (Figure 32)

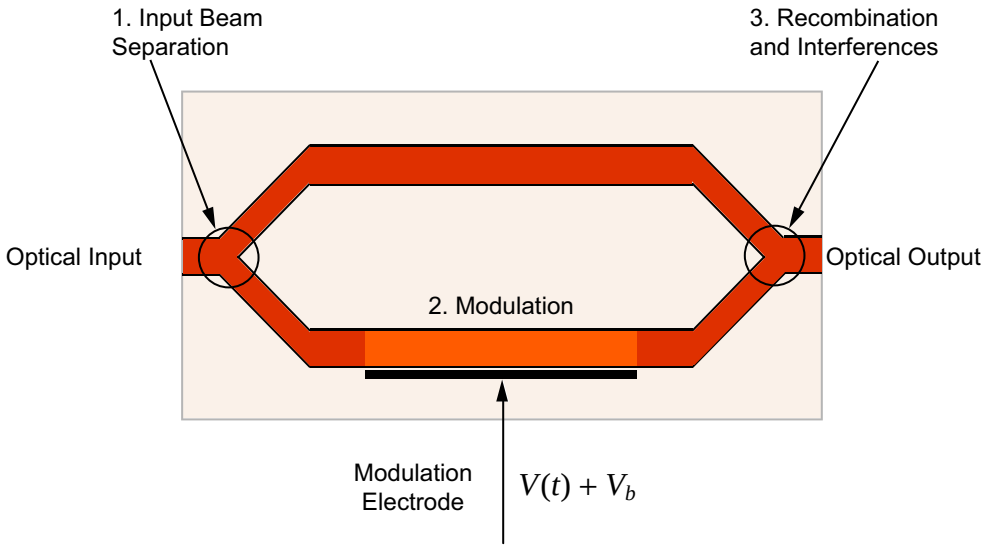


Figure 31: Functional diagram of a Mach-Zehnder modulator.

voltages than for their X-cut counterparts. On the other hand, X-cut modulators are chirp-free. For our application, we preferred a lower half-wave voltage to no chirp. Therefore, we chose Z-cut modulators.

The modulator output optical power P_{out} is a function of the modulation voltage $V(t)$ as given by

$$P_{out}(t) = P_0 \cos^2\left(\frac{\pi V(t)}{2V_{\pi,RF}} + \phi\right) \tag{25}$$

where ϕ represents the fixed phase shift associated with the operating point, $\phi = \frac{\pi V_b}{2V_{\pi,DC}}$ and $V_{\pi RF}$ and $V_{\pi DC}$ represent the dynamic and static half wave voltages of the modulator. The modulator operating point is set by the voltage V_b applied to the DC bias electrode [84].

The transfer function of a modulator presents extrema, points where the output power is either maximum or minimum (almost zero). A maximum output power corresponds to constructive interference at signal recombination (#3 in Figure 31): the amplitudes of the two in-phase signals add. The other type of extrema corresponds to destructive interference. The two signals are perfectly out of phase and cancel at recombination. The ratio of output powers for destructive and constructive interferences is called the extinction ratio, which is greater than 20 dB for our modulators.

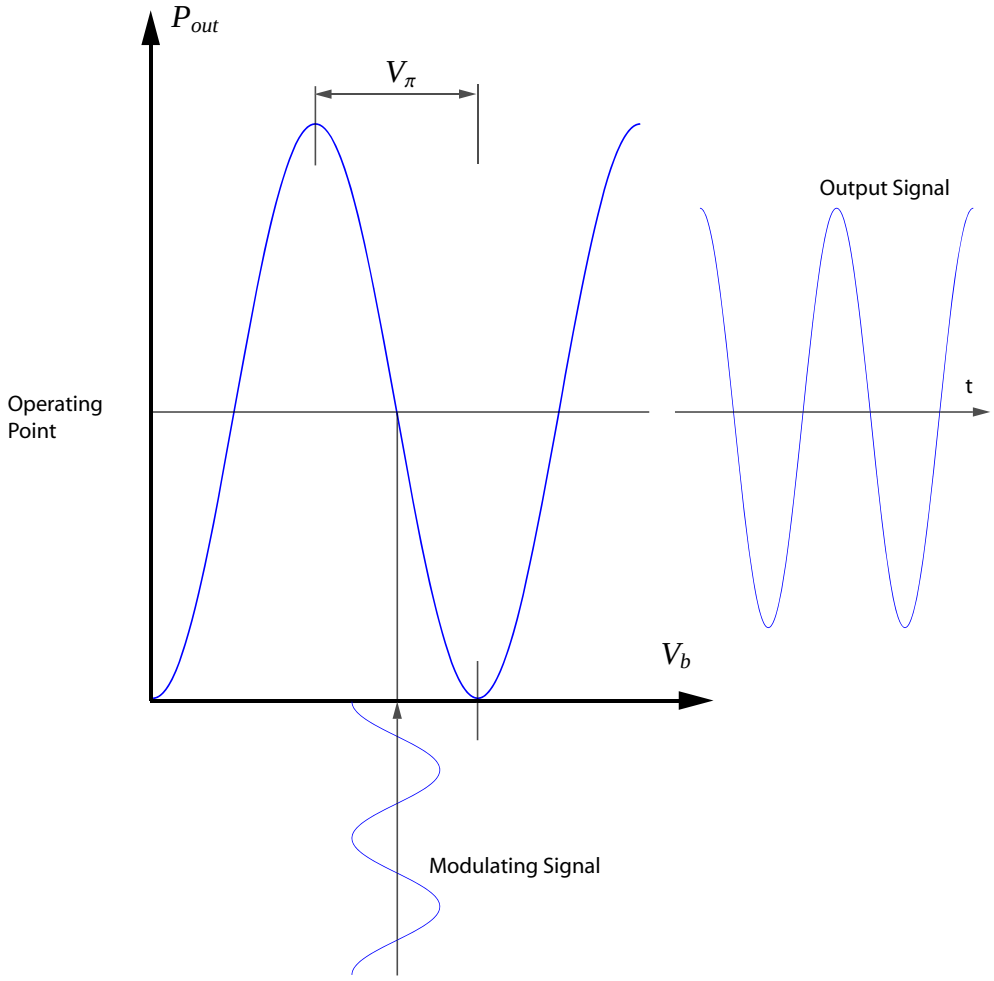


Figure 32: Modulation in a Mach-Zehnder interferometer.

The voltage difference that separates two successive extrema of the non-linear function is called half-wave voltage V_π, as illustrated in Figure 32. A low V_π indicates a better quality modulator as a lower voltage applied to the modulation electrode is sufficient to go from one extrema to the next. The half-wave voltage was measured experimentally as 4.2 V for our modulators. Typical V_π values from other brand components lie in between 5 and 6 V.

The modulator is an opto-electronic component and, as such possesses a very wide (yet limited) bandwidth. This bandwidth limits the maximum modulation speed and, therefore, limits the maximum communication bit rate. The bandwidth was measured experimentally on the purchased modulators by way of their electro-optic response (Figure 33). Since

we are searching for "twin" components, we were able to verify the good match of the characteristics. The electro-optic responses are always within 0.5 dB of each other over frequencies ranging from DC to 12 GHz. This bandwidth is sufficient for our current bit rate objective. This fundamental component is also available with bandwidths up to 40 GHz [82].

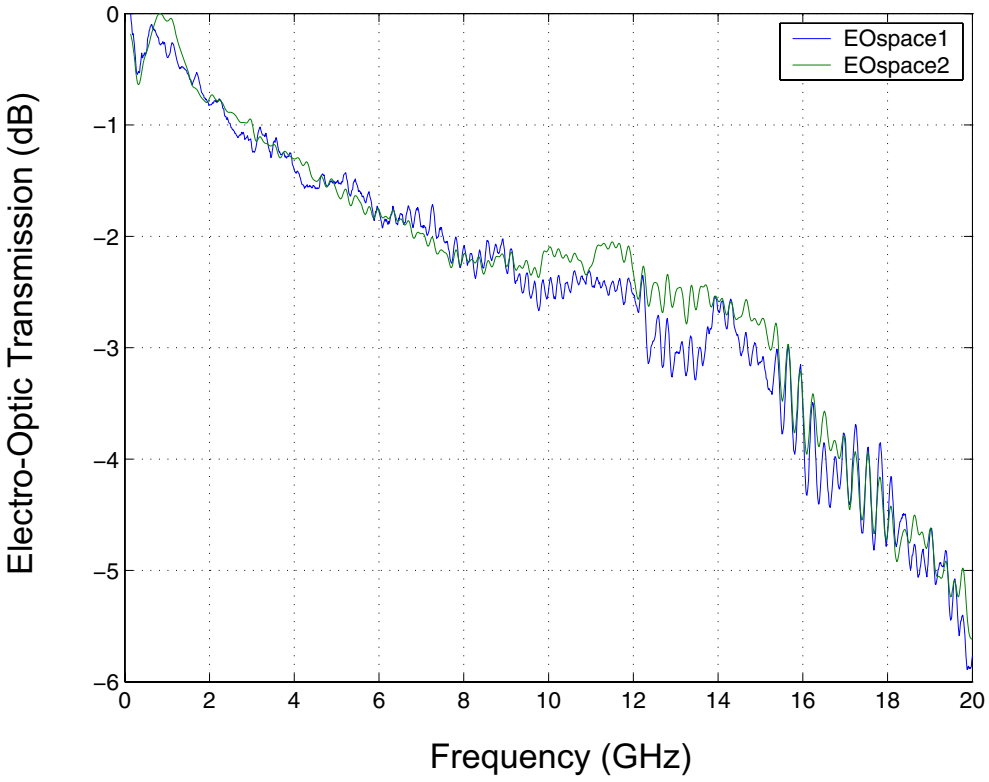


Figure 33: Electro-optic modulator transmission as a function of frequency.

The modulator is the non-linear element of the system. We also investigated the $\cos^2$ non-linear function and the match between our two modulators (Figure 34). We observe two similar profiles for the transfer functions, with only a 0.7 V shift in between the two. Experimentally, this difference is easily compensated by shifting the DC bias voltages, to set the operating point at the same location for the respective transfer functions.

To present the full characteristics of the modulators, we need to mention the optical insertion losses and the extinction ratio. The insertion losses, expressed in dB, are the losses in optical power of light passing through the component in a constructive interference setup.

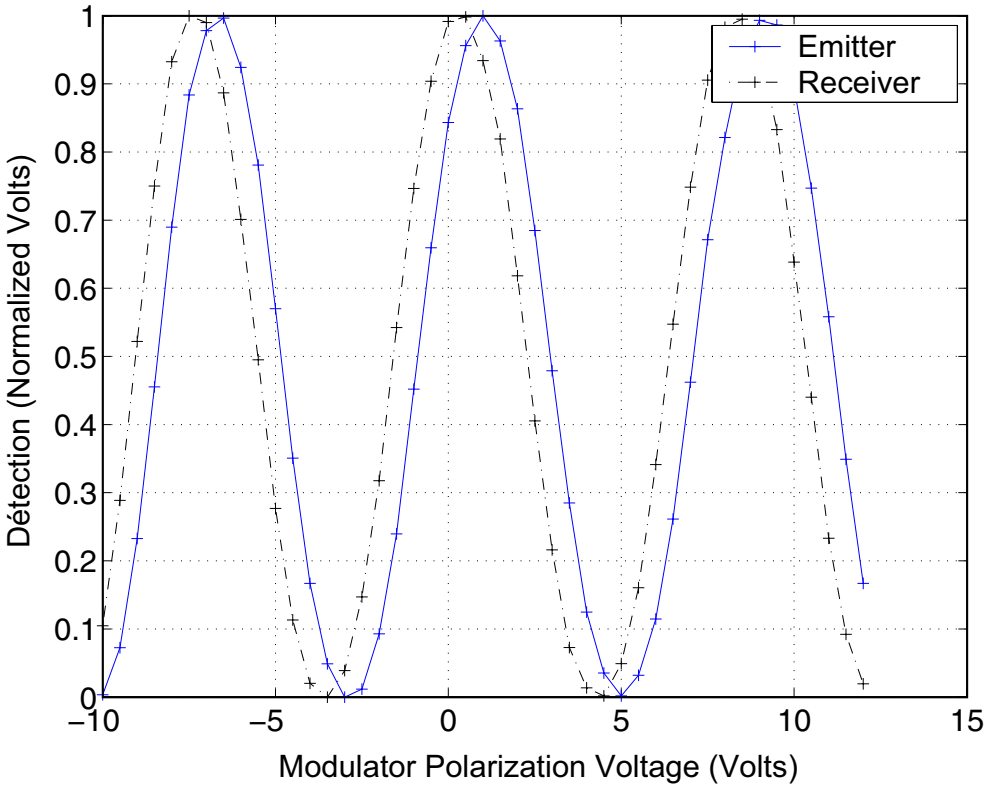


Figure 34: Normalized open-loop electro-optic transfer function.

Obviously, lower losses are best. We measure experimentally losses of 1.6 dB for EOspace modulators, whereas competitor product losses are between 3 and 6 dB. The extinction ratio is measured to 20 dB.

Therefore, we are in possession of two high quality modulators, non-linear components around which we have built our system. Having quality "modulator-driver" pairs with very close impulse responses (Figure 35) is important. These two transmission plots do not evidence any blatant difference in opto-electronic gains between those two component pairs. Without directly launching into the mismatch study presented in Chapter 4, the closeness of these plots is important to achieved good synchronization results.

3.2.1.5 Delay line

The delay in the emitter is created by inserting a six meter length of SMF 28 fiber. To determine the minimal time delay necessary for the generation of high complexity chaos,

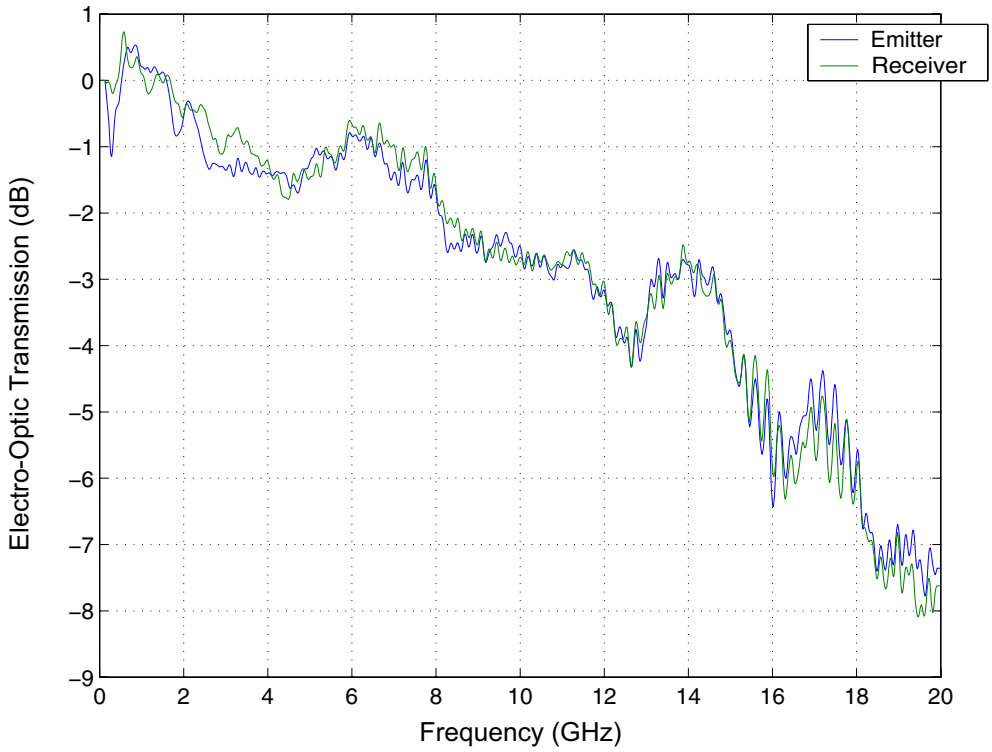


Figure 35: Electro-optic transmission as a function of frequency.

we base our calculations on a time-honered empirical rule: the delay needs to be at least ten times greater than the time constant associated to the highest system frequency. Since the high frequency cutoff of the system is close to 6.5 GHz, the delay needs to be greater than $(10 * 1/(2\pi \cdot 6,5 \cdot 10^9)) = 245$ ps. The total delay of the emitter feedback loop is the combination of the light propagation time through the optical fiber and the propagation time of the electrical through the RF components. The overall system delay is measured in Section 3.2.2.2 and is of the order of 40 ns, well above the empirical limit and confirming our capability of generating chaotic regimes whose attractor dimension is several hundred [25].

Simple fiber suffices at the emitter to create the delay, but, at the receiver, the exact delay matching that needs to be achieved poses a bit of a technical problem. We will study this further in Section 4.2.2, but, when selecting components, we needed picosecond delay adjustability. To achieve this, we opted for a variable fiber delay. With a precision of ±0.02 ps and a repeatability of ±0.02 ps, the variable fiber delay from General Photonics is

perfectly adapted for the task.

3.2.1.6 Message

The message is a binary zero-average electrical signal of peak-to-peak amplitude 2 V. This signal drives a direct-modulated NEL laser diode, NLK5CE2KA. With a maximum bit rate of 10 Gb/s, the NEL diode is fast enough for purposes. The laser diode, with a threshold current of 10 mA, is polarized by a 33 mA current. On a 50 Ω line, the message becomes 40 mA current fluctuations. Therefore, for a '0' bit, the laser diode is almost off. For a '1' bit, the laser diode is driven by a 50 mA current. This corresponds to an optical output power of 0.5 mW. A variable optical attenuator controls the optical power that is really inserted into the chaotic feedback loop. This attenuator acts directly on the α parameter (Equation (24)) and hence, on the message masking rate within the chaotic transmission. We will encounter this parameter again in Equation (29) and for a more in-depth study in Chapter 4, Section 4.2.3.

The message is inserted inside the optical feedback loop by a 2x2 optical coupler (Figure 36). This passive optical component sums the two input intensities and outputs half of this sum on each of the output branches. The polarization of the two laser sources (DFB and direct-modulation lasers) are set to be orthogonal to avoid interferences in between the signals as we want an intensity sum without interference terms.

3.2.1.7 System cost

Aside from the purely scientific aspect of this research, the economics need also be considered. Table 2 presents the list of components and their prices, to estimate the necessary investment needed to duplicate the system. We have not included in this table the cost of optical fiber, whose cost in negligible when compared to the other components.

At this point, we are in possession of an oscillator based on a principle that can generate, under certain conditions, chaotic oscillations. We need to identify the conditions that need to be met for chaotic oscillations, and, therefore we need to identify the range of parameter values necessary for chaotic dynamical regimes. We will also characterize our experimental

Table 2: Summary of system component costs

System component	Unit price (€)	Quantity
Alcatel 1905LMI DFB laser diode	1600	2
EOspace electro-optic modulator	8998	2
SHF RF amplifier	10300	2
Variable fiber delay line	6435	1
Miteq photoreceiver	3000	2
NEL direct modulated laser diode	3000	1
Laser diode controllers and mounts	11755	3
Total (€)	69006	

setup within the framework of optical communication.

3.2.2 Experimental implementation

Two steps are necessary to finalize the chaotic emitter of this system. This first one is the identification of the range of parameter values that generate chaotic behavior. The second step is the characterization of the emitter and the determination of its properties that are of special interest to us with respect to cryptography and communication, further developed in Chapter 4, Section 4.2.3.

3.2.2.1 Emitter setup

The experimental implementation proceeds directly from the diagram of Figure 27. We use the components described in Section 3.2.1 organized in a closed loop to form the chaotic emitter. The component layout is described at Figure 36.

The experimental diagram of Figure 36 is very close to that of the original intensity chaos setup described by Figure 21. The first difference is the greater bandwidths of the components we have used. But the most important difference between the two setups is the positioning, inside the chaotic feedback loop of the message insertion.

Pascal Levy electronically inserts the message into the feedback loop via a power divider, used here as an adder [62]. The adder is placed between the RF amplifier and the electro-optic modulator. The problems stemming from this technique are twofold. Firstly,

the power divider introduces high losses, on the order of 6 dB, in the feedback loop, limiting the maximum modulation signal power to, at most, half of the RF amplifier output signal. This loss severely limits the number of non-linearity extrema that are being swept, and, therefore, also limits the complexity of the dynamics. Secondly, the message is inserted in electronic form. The message bandwidth is, therefore, limited to the electrical spectral bandwidth of the chaotic carrier to guarantee proper masking.

We have chosen to insert the message optically right before the detection and amplification. From the placement of the optical coupler, the losses can be compensated by increasing the optical power output from the continuous wave laser diode. This way, the RF amplifier maximum output power is easily reached. The system can sweep a maximum number of non-linearity extrema for a maximum complexity chaotic dynamic.

Tho optical message insertion also presents an advantage from a message bandwidth perspective. The maximum message bit rate is now subject to the optical spectrum of the chaos at the electro-optic modulator output. This optical spectrum results from the spreading of the electrical chaotic spectrum as the signal traverses the highly non-linear component into the optical domain. The optical signal at the output of the modulator is, therefore, much broader than the electrical input, allowing for the masking of messages with wider spectra, without modifying the chaotic electrical spectrum. The combination of these two advantages made us opt for a message insertion right before the detection and amplification as presented in Figure 36.

The emitter, built at GTL-CNRS Télécom, in Metz, France, is composed of the following elements, identified by number, in Figure 37:

1. An electro-optic Mach-Zehnder Interferometer (MZI) that acts as an intensity modulator. The operating point is set by the DC bias voltage V_{B1}. The interferometer is illuminated with power P_1 by a CW DFB laser operating at the 1550nm wavelength,

2. A length of fiber performing a pure delay on the signal output of the MZI. The fiber delay time is on the order of 40 ns.

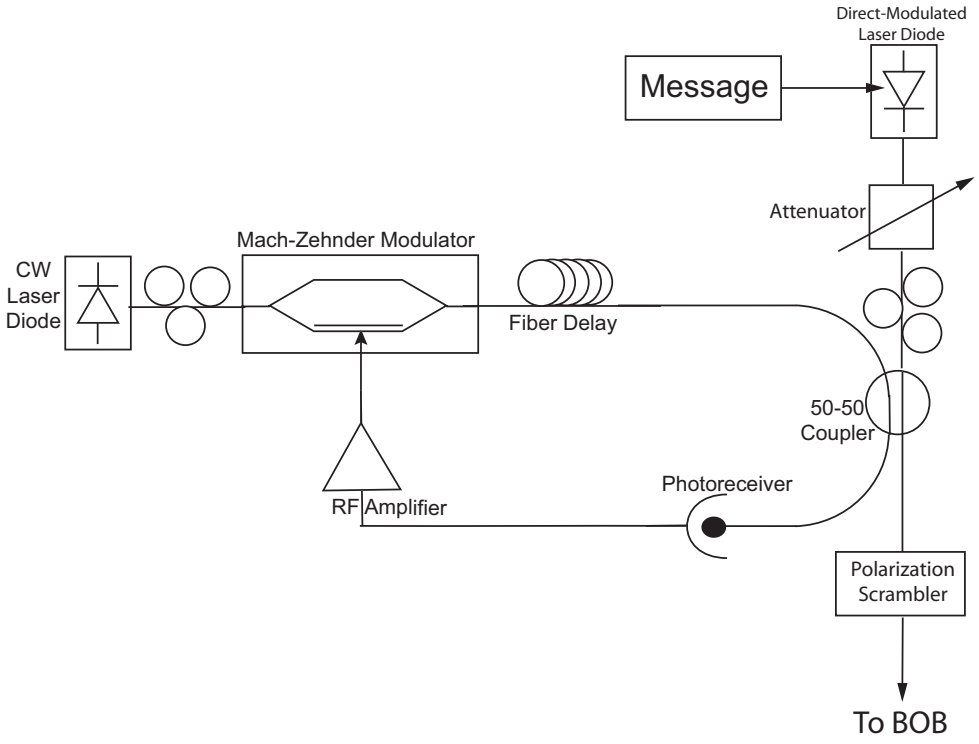


Figure 36: Experimental emitter schematic diagram.

3. A 2x2 fiber coupler allows mixing an information message, transmitting a part of the message hidden in the chaotic optical signal, and feeding the complementary part of the same encrypted chaotic optical beam back to the Mach-Zehnder.

4. A 2 V/mW photoreceiver and an 18 dB gain radio-frequency (RF) amplifier to convert the feedback optical signal into an electronic one, which is applied to the Mach-Zehnder RF electrode. High gain and high RF power amplifiers are required to force high-complexity chaotic behavior in the emitter oscillation loop.

5. A 10 Gbit/s direct-modulated laser diode operating at 1550 nm manufactured by NEL. The message generated at the modulated diode is injected into a tuneable optical attenuator to control the message amplitude within the feedback loop. By adjusting the attenuator, we can ensure that the message does not stand out in the transmission. A polarization controller is used before the message addition coupler to ensure a non-interfering light superposition in the coupler through a cross polarized light

beam (i.e. light intensity addition instead of amplitude addition). To prevent separation by an eavesdropper between the chaos and the signal light beam though a simple polarizer, an integrated polarization scrambler can be used at the emitter output.

For easy system modeling, we consider a second order band pass filter function, which comprises first order low pass and high pass filters.

The Fourier transform of a low pass filter transfer function (output/input) is:

$$\frac{output}{input} = \frac{1}{1 + p\tau_1}, \tag{26}$$

and that of a high pass filter transfer function is:

$$\frac{output}{input} = \frac{\frac{p}{\tau_2}}{1 + \frac{p}{\tau_2}} \tag{27}$$

where τ_1 and τ_2 are defined in Equation (30).

The multiplication of those two transforms gives the bandpass filter transfer function:

$$\frac{s}{e} = \frac{\frac{\tau_1}{\tau_1+\tau_2}}{1 + p(\tau_1 + \tau_2) + \frac{\tau_1\tau_2}{\tau_1+\tau_2}\frac{1}{p}}. \tag{28}$$

By taking the inverse Fourier transform of this expression and replacing the terms of Equation (23) by the adopted models, we obtain the following equation for the emitter:

$$x(t) + \tau\frac{d}{dt}x(t) + \frac{1}{\theta}\int x(t)\,dt = A\left[\cos^2[x(t-T) + \phi] + \alpha m(t)\right] \tag{29}$$

where $m(t)$ denotes the message to be transmitted, T the time delay, and ϕ the phase parameter that controls the MZI operating point. The following parameters need to be defined:

$$\tau_1 = 1/2\pi f_1, \tag{30a}$$

$$\tau_2 = 1/2\pi f_2, \tag{30b}$$

$$\theta = \tau_1 + \tau_2, \tag{30c}$$

$$\tau = \tau_1\tau_2/(\tau_1 + \tau_2), \tag{30d}$$

$$A = \pi P_0 S G/2V_{\pi RF}, \tag{30e}$$

$$\phi = \pi V_b/2V_\pi, \tag{30f}$$

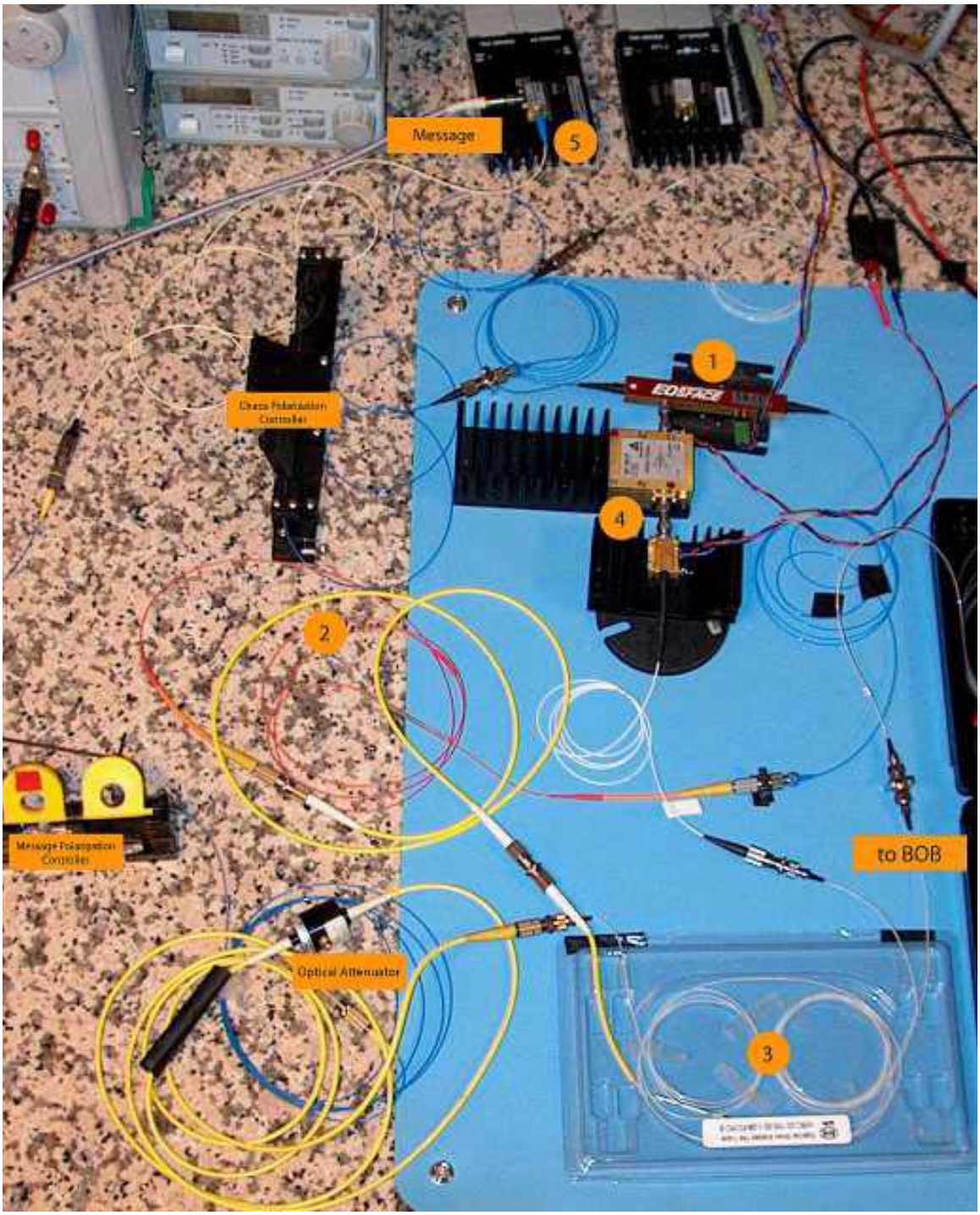


Figure 37: Picture of the opto-electronic emitter setup.

where f_1 and f_2 are the respectively high and low cutoff frequencies of the bandpass filter, and A the gain of the opto-electronic feedback loop. The parameter A is the bifurcation parameter of the system that modifies P_0, the optical power output of the continuous wave laser diode.

The method of inserting the message into the chaotic feedback loop is termed additive chaos modulation and is described in Section 3.1.2. Half of the message power is inserted into the feedback loop and contributes to the chaotic dynamics of the emitter. The other half is added, in clear text, to the transmission signal. Therefore, the masking of the message inside the transmission signal is dependent on the small amplitude of the message as compared to that of the chaotic carrier (α factor) and the carrier wave that is also a function of an earlier message value (T seconds earlier).

To insure transmission security, on top of the masking, we must guard against an eavesdropper optically separating the message from the carrier. Consequently, special care is taken to have the laser wavelengths be very close (no more than a few GHz apart). Also, since the two laser polarizations are orthogonal, we have to insert a polarization scrambler to avoid easy separation of message and carrier by a polarizer.

3.2.2.2 Experimental delay measurement

The delay introduced at the emitter plays an important role in the system security. Inserting a delay increases the dimension of the system phase space for a greater generated chaos complexity. But mostly, as we will see in Section 4.2.2 in the next chapter, this parameter is the factor that necessitates the most precise and accurate tuning. The influence of mismatch in delay on communication quality is very high.

The delay was measured by launching an electrical pulse in the chaotic feedback loop and measuring the pulse's propagation time. The pulse successively propagates through the RF amplifier, the modulator, the delay line, the 2x2 coupler and the photoreceiver. The vectorial network analyzer generates the pulse and also handles the visualization (Figure 38). The measurement gives an emitter delay of 42.15 ns, which is the value that will have to

be approached as best possible for good parameter tuning. The precision that is necessary at the receiver is linked to the lower system time constant τ. Indeed, the high speed fluctuations of the system are of the order of τ, with variations between emitter and receiver on the order of $\Delta\tau$. Therefore the maximum deviation for the delay matching is also on the order of $\Delta\tau$.

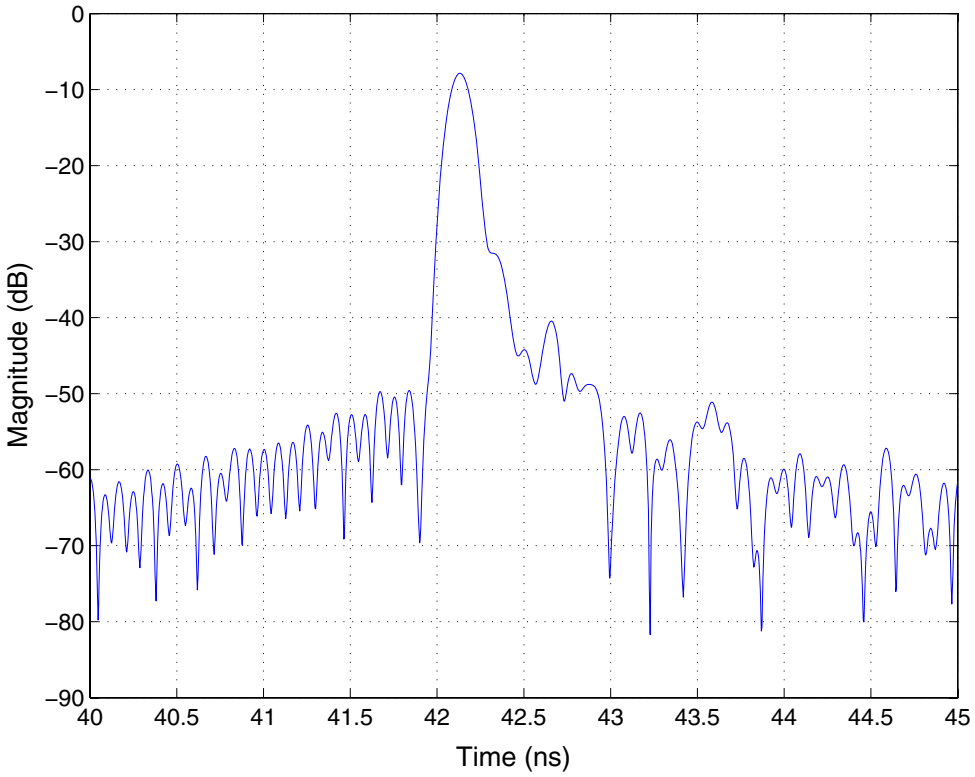


Figure 38: Experimental measurement of the emitter delay.

3.2.2.3 Bifurcation

With the emitter architecture and components that have been described above, we need to verify that the system behaves chaotically under certain conditions, and we need to identify those conditions. This verification and identification are both done by plotting the system bifurcation diagram.

Depending on the situations, different plotting methods can be used [62]. In some cases, the spectrum is plotted as a function of the bifurcation parameter. In other cases,

the probability density function of the signal amplitude is represented as a function of the bifurcation parameter. In our case, we chose the system gain A as the bifurcation parameter. From Equation (30e), the gain A is directly proportional to the optical power P_0 of the continuous wave laser diode.

The bifurcation diagram was constructed using the laser diode power as a bifurcation parameter. Time traces of 100000 points were recorded for laser diode powers ranging from 0 mW up to 7 mW, with 0.125 mW increments. The MZI bias voltage was set to $V_{B1} = 5.69V$. From these time traces, the probability density function was constructed, and the amplitude normalized. The result is the bifurcation diagram presented in Figure 39. In

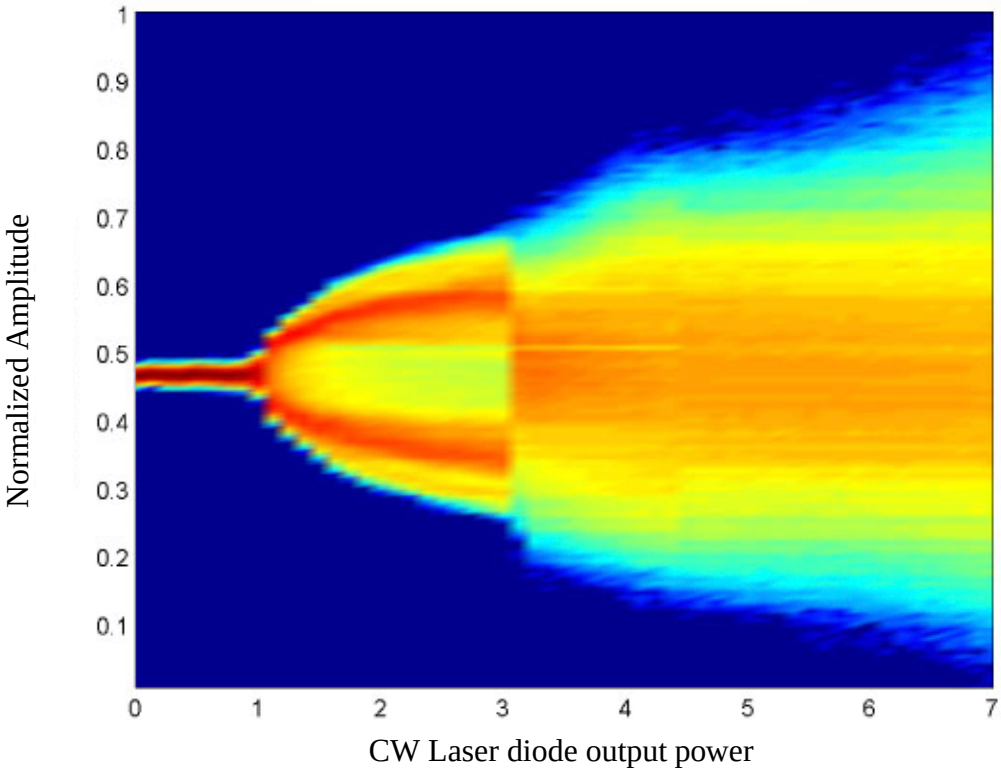


Figure 39: 2D experimental bifurcation diagram.

this figure, we clearly see the original periodic oscillations for a laser diode power ranging from 0 to 1 mW. At this point, there are two distinct paths that separate up to $P_1 = 3$ mW: one in the lower amplitudes and the other in the higher amplitudes. We can also witness

the evolution in the dynamics by looking at the time traces of the system at different optical powers. The time trace in Figure 40a presents oscillations of very small amplitude, closer to noise than to proper oscillations. As the CW laser diode power is increased to 1.25 mW, we go beyond the first Hopf bifurcation [12], and the first oscillations appear (Figure 40b). This bifurcation changes qualitatively the oscillations of the system, from a fixed point to periodic oscillations. This is what we observe on Figures 40b and c. The oscillation amplitude increases but not their general aspect.

At $P_1 = 3mW$, there is a crisis, a sharp discontinuity in the amplitude distribution. Then, as P_1 continues to increase, the Gaussian amplitude distribution centers around normalized amplitude 0.5 and spreads to span the full amplitude range. This brutal rupture in the dynamic is transition between a certain periodicity and a chaotic-type regime (evidenced by predominant non-linear interactions). We will not study in further detail the periodic dynamics because this is not the focus of this thesis. We will consider that after 3 mW, the system oscillations are chaotic. Based on this observation, we will operate the CW laser at output powers ranging from 5 to 7 mW, well within the chaos zone.

By plotting the bifurcation diagram of Figure 39 in three dimensions, we can observe the form of the PDF function. The laser diode power and oscillation amplitudes axis remain the same. The vertical axis represents the value of the PDF in arbitrary units (linear scale).

One of our objectives is to obtain a neutral signature chaos. From a statistical standpoint, the most neutral is the Gaussian white noise. To verify the similarity of our system behavior to a Gaussian, we computed the coefficients of Gram-Charlier (Figure 6 of [17]) from experimental time traces obtained for different laser output powers. The first even and odd coefficients (a_3 and a_4) go to zero once the optical power has reached 4 mW. For an optical power of 7 mW, the PDF was constructed and compared to the corresponding Gaussian PDF (Figure 7 of [17]). The experimental PDF deviates from the Gaussian one mostly at the tail ends of the distribution. The Gaussian distribution is very visible on the 3D plot of the bifurcation diagram (Figure 41).

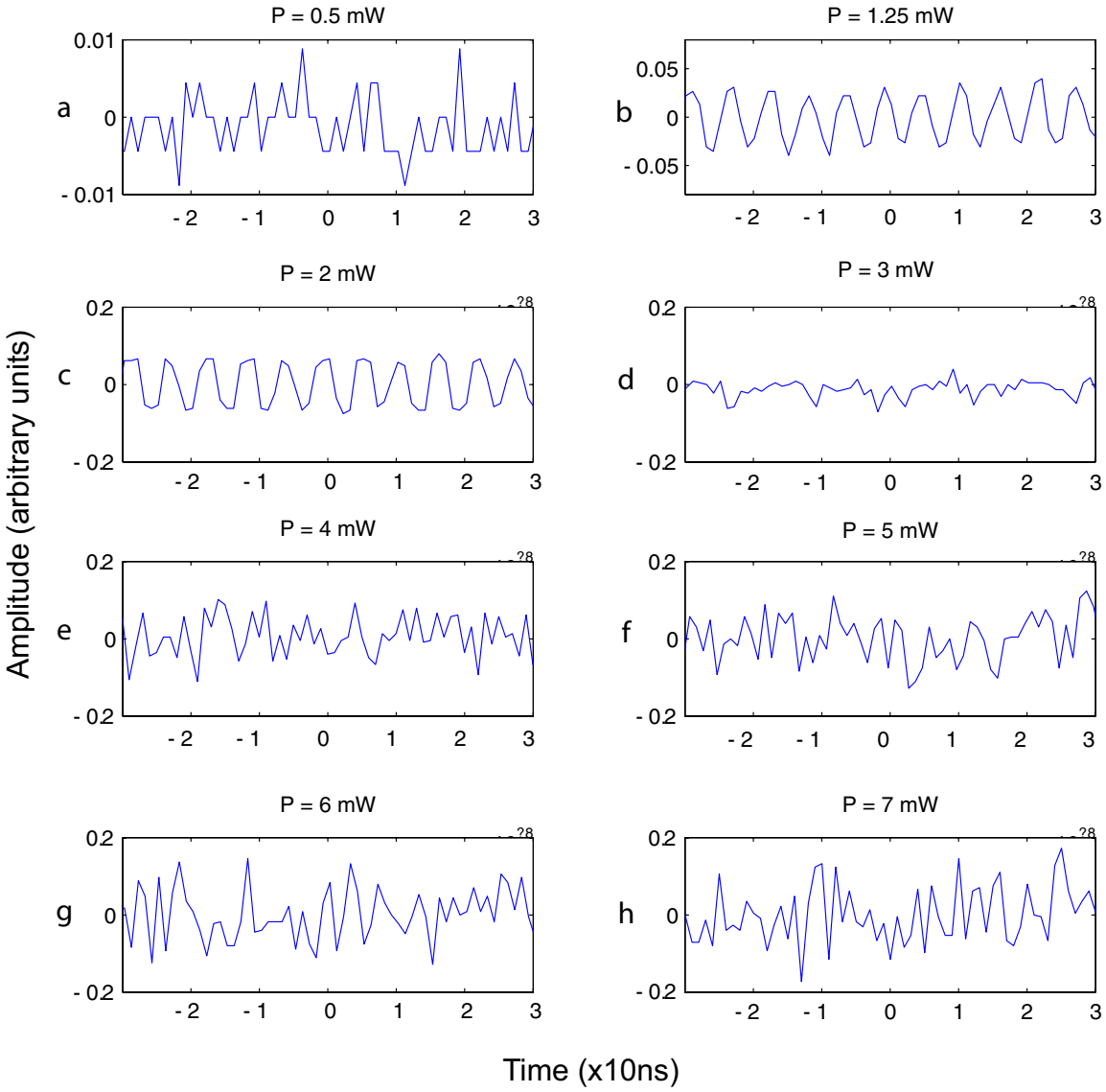


Figure 40: Time traces for different optical powers.

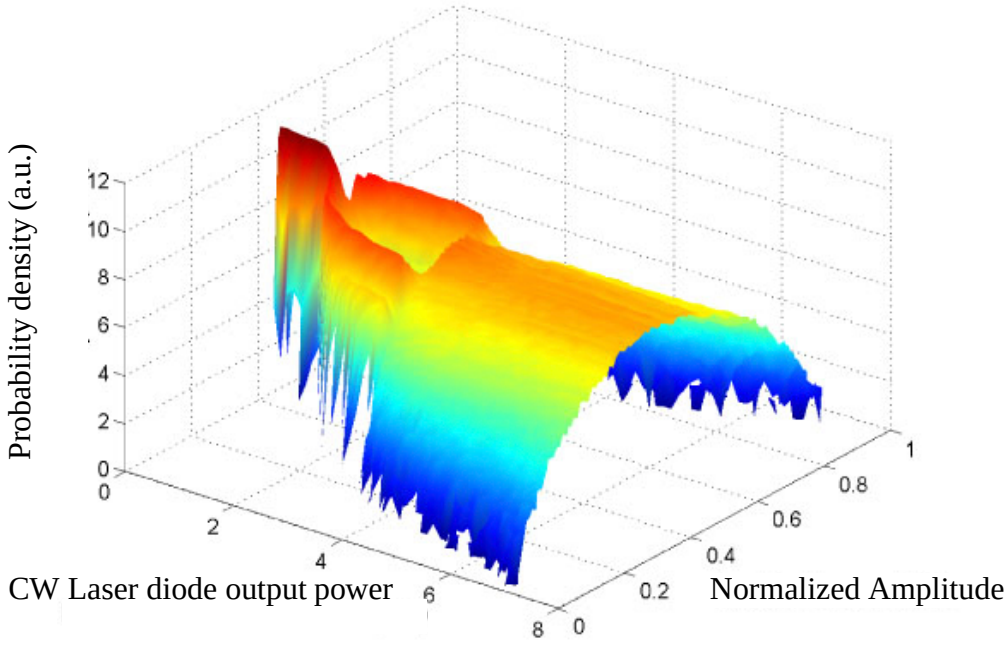


Figure 41: 3D Experimental bifurcation diagram.

The white noise property that we are looking for is the constant spectrum level over the considered frequency range. Clearly, a physical system does not have an infinite bandwidth, therefore the term "white noise" is used by extension because of the very wide spectrum (from tens of kHz to multiple GHz). We verify this by studying the spectrum, both electrically and optically.

3.2.2.4 Spectra

From the bifurcation diagrams, we have determined the parameter range for chaotic oscillations. When the system is oscillating chaotically, we now measure the electrical spectrum of the system to estimate the −3 dB bandwidth. We also measure the optical transmission spectrum to determine the optical bandwidth that the system would occupy in a fiber network.

Electrical Spectrum From the electrical spectrum observation, we can measure the cutoff frequencies, taken 3 dB below the maximum power of the signal. We will consider that the spectral bandwidth useful for the spectral masking of a signal is between these

two cutoff frequencies. The lower frequencies are filtered by the RF components of the emitter and therefore do not appear in the spectrum. The electrical spectrum is measured at the output of the photoreceiver with a 40 Hz to 22 GHz electrical spectrum analyzer. The lower cutoff frequency is around 30kHz and the upper cutoff frequency is around 6.5 GHz for a system bandwidth of 6.5 GHz. The element that limits the bandwidth of the system is the photoreceiver. The trade-off is that this element shows a very high gain for the optic to electronic conversion. The gain is necessary to obtain high-order chaos.

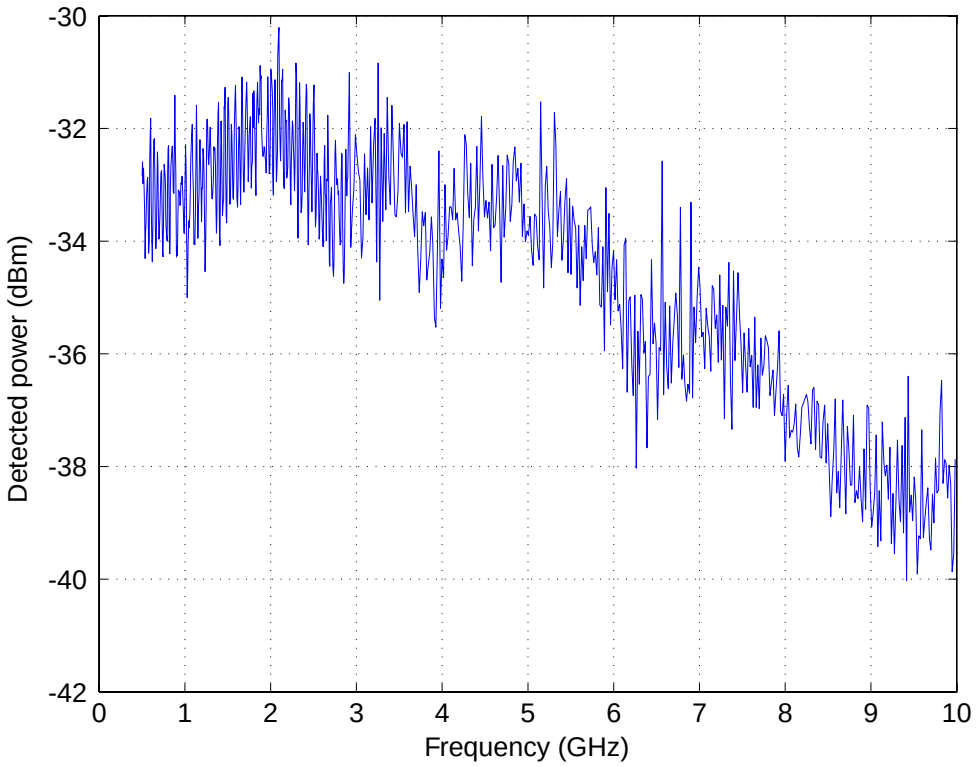


Figure 42: Electrical experimental chaos spectrum.

Optical Spectrum Figure 43 presents the optical spectrum measured on the transmission line (the "to Bob" path in Figure 36) for various laser diode output powers (P_1). These data points were collected with an Anritsu optical spectrum analyzer of 0.07 nm resolution. The purpose of this measurement is to provide a measure of the required channel bandwidth for a future telecom implementation.

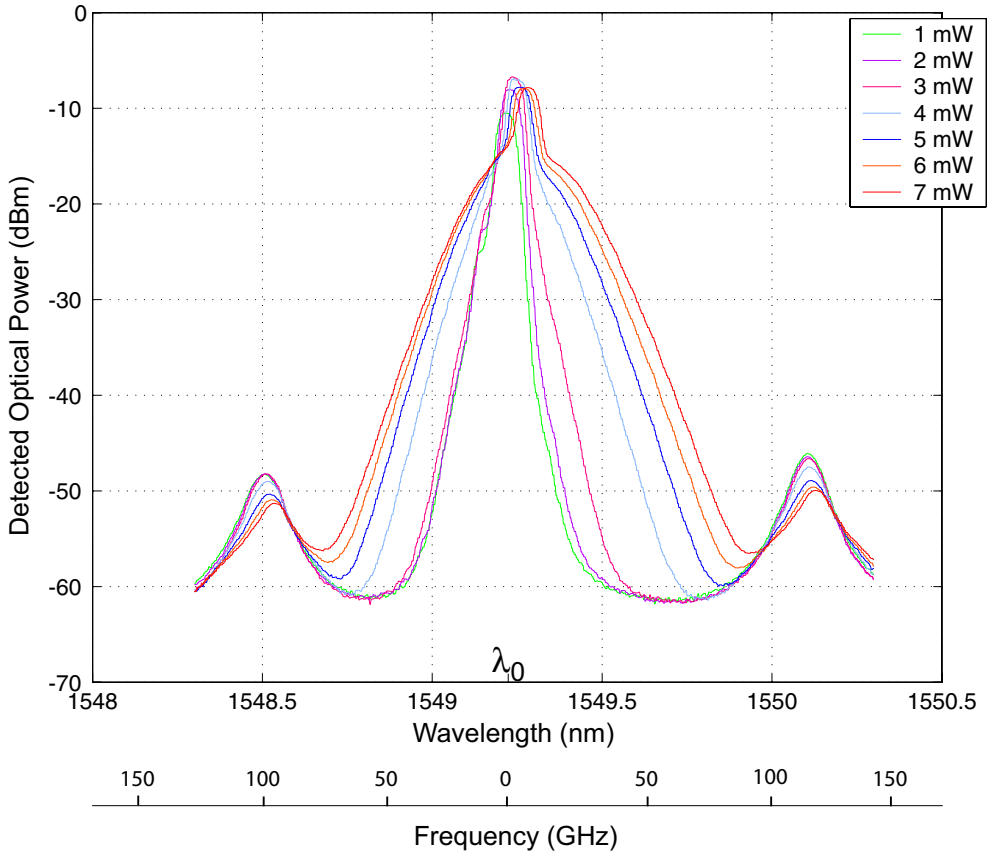


Figure 43: Optical transmission spectrum for various laser diode output powers (P_1).

The optical spectrum of the transmission signal presents the shape of a monomode ray when the laser power is below 3 mW. As the optical power increases, we see an important optical spectrum broadening, while conserving an important central peak which stands out by about 5 dB_{OPT}. The spectrum broadening can reach 0.2 nm. This measure is taken 3 dB_{OPT} below the maximum modulation level (without considering the central peak) and corresponds to a bandwidth of 25 GHz. For a laser power of 7 mW, the emitted signal is broader than the 0.8 nm typically allocated for each channel. For a network implementation of this system, it will be important to allocate at least 1.6 nm. Another possibility would be to limit the electrical bandwidth of the system to have the optical spectrum fit within the allocated channel space, keeping in mind the correspondence between optical decibels and electrical decibels; the electrical decibel scale is double the optical one.

Conclusion

The first chapter provided a better grasp on the notion of chaos, the reasons for using chaotic dynamics in telecommunications and the experimental realizations in the field. In this second chapter, we detailed the chaos generator principle, stemming from the intensity Ikeda setup (Section 3.1). This principle, already present in previous work [62], is expanded on in our work. The different methods of inserting the message into the transmission are described (Section 3.1.2). We chose to implement the chaos modulation technique.

The details of the components and the operations of the experimental chaos cryptography system are described in Section 3.2. The different criteria for the selection of each components were listed and each evaluated based on their characteristics: the opto-electronic modulators for their bandwidth, their half-wave voltage and their insertion losses; the RF amplifiers for their bandwidth, gain and maximum output power; the photoreceivers for their opto-electronic conversion gain. During this process special attention was paid to matching components with the future implementation of the receiver in mind (Section 4.2.2).

The oscillator was characterized by its optical, electrical spectra and by bifurcation diagrams. By plotting the bifurcation diagram as a function of the detected optical power, we determined the chaotic operating range of the oscillator. By using the spectrum plot tool, we found the frequency limitations a message would have to have to be properly encrypted. For a WDM network deployment, the optical spectrum plot gave a measure of the occupation of the signal on an optical fiber during transmission. With this information, the necessary WDM channel spacing is measured.

At this point in the dissertation, we have in our possession a non-linear system that can, under certain conditions, oscillate chaotically, producing a broadband, 6 GHz bandwidth chaotic signal. This oscillator will serve as the emitter within the complete chaos cryptography communication system. The receiver will be studied, with special emphasis on its adaptation to the emitter. The overall system performances (BER, masking) will be

detailed in the next chapter.

CHAPTER 4

TOWARDS A CRYPTOGRAPHIC SYSTEM

In this chapter, the communication system is completed with the addition of a receiver. Under certain conditions, the receiver is capable of decoding the message inserted into the transmitted signal. The cryptographic nature of the transmission is insured by the difficulty in finding and bringing together the conditions necessary for the proper reconstruction of the information.

This chapter will first explore the cryptographic context, both the software and the system approach. Secondly, we will detail the decoding principles of cryptographic systems and determine the optimal operation of the receiver. Finally, the complete system, emitter-receiver, will be tested to evaluate decryption performance.

4.1 Cryptography notions and context

The three characters Alice, Bob and Eve are still at the forefront of our study. Alice and Bob want to communicate. Eve is trying very hard to find out the text of their communication: she is listening to the information transfer. Alice and Bob want their conversation to remain secret. For this, they have at their disposal a panel of cryptographic methods, both system and algorithm based.

A first approach, called steganography, consists of hiding the message inside a message with no obvious secret characteristics. A practical implementation took place in ancient Greece. A message was tattooed on the shaved head of a slave. Once the hair had grown back, Alice's slave would travel to Bob. His head, again shaved, would reveal the message to Bob, thus establishing secret communication.

A second approach consists in transforming the message so a spy with access to the transmitted information cannot decipher the transmission content. We call this approach cryptography. Different methods, involving different principles and technologies, have

been developed to meet different security needs.

The security of the first approach is based on a coding algorithm. The information is encrypted before transmission. The algorithm, usually known, makes use of a secret encryption key. The secret nature of this key restricts information access to authorized receivers. This key is said to be symmetric when the same key is used for both encryption and decryption. This principle is implemented in the Data Encryption Standard (DES) as shown in Section 4.1.1.1.

The key can also be double, with a public part, and a private part. The keys to encrypt/decrypt are generated by combining the public and/or private keys of both Alice and Bob. The result of this combination is unique to an exchange between Alice and Bob, known only to the two of them. An example of a public key - private key encryption system is RSA,[1] which explained in Section 4.1.1.2.

The complexity of the mathematical modeling and of the reverse calculation of the algorithm make any non-authorized attempt at deciphering extremely complicated. The implementation of this form of cryptography can be done by software or with special-purpose chips.

The second cryptographic approach that we will describe relies on security based on physical principles to insure the confidentiality of the message. These principles cannot be implemented with software, only by physical systems. Indeed, there is no binary signal that is directly accessible: a minimum of physical means are necessary for access to the physical data flow, which can then be processed. We call this method a "system" approach, and this type of encoding will be further expanded on in Section 4.1.2.

Another problem very present that has not been touched upon so far is the authentication of the receiver. To put it simply: "Is it really Bob that is receiving our message ?" On top of making the message secure during transmission, authentication of the receiver that

[1]Named after its inventors: Rivest, Shamir and Adleman.

is obtaining, through the key, the means to decipher the message is necessary. The cryptographic aspect of our system is focused on securing the transmission, not on distributing the key. We will see how other methods can complement chaos cryptography by authenticating the receiver.

4.1.1 Software approach

There are many algorithms available to encrypt data. We will detail the workings of two specific algorithms to illustrate symmetrical key encryption and public key - private key methods. We will see how the two example schemes (DES and RSA) combine within the commercial software Pretty Good Privacy (PGP) to provide a complete system with both key distribution and encryption.

4.1.1.1 DES

In 1972, the National Bureau of Standards, know today as NIST, wanted to promote a secure encryption scheme for non-military applications. An IBM research group proposed the algorithm known today as DES, which became a standard adopted by ANSI in 1981 [10].

The operation of the DES cypher is presented in Figure 44. This cypher operates with 64 bit text blocks, the entire message being broken up this way. Each bloc is then divided into two 32 bit blocks, L_0 and R_0, shown as the left and right hand blocks in Figure 44. Sixteen iterations of the same operations yield the cyphertext. The ith iteration combines the left hand block, L_{i-1}, the right hand one, R_{i-1}, a bit permutation function 'f', and a key K_i to generated the next blocks L_i and R_i. The algorithm can be summarized by Equation (31) of which 16 iterations yield the cyphertext:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i), \end{aligned} \tag{31}$$

where $\oplus$ represents the logical XOR operation.

The function 'f' combines the message block R_{i-1} with the key K_i with the following process: firstly, R_{i-1} is extended from 32 to 48 bits. All the bits are flipped and some bits

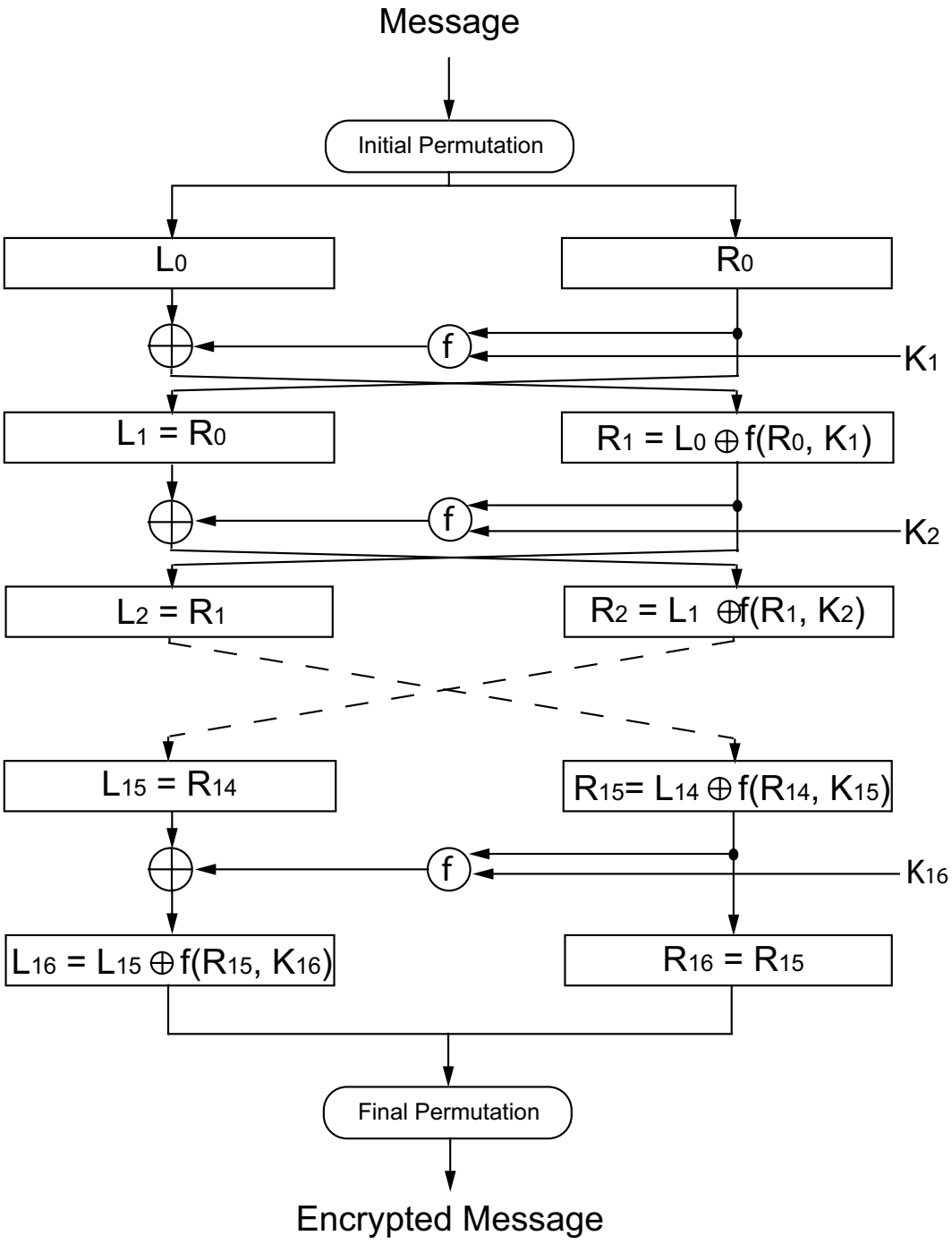


Figure 44: DES principle diagram.

are repeated following a known and constant scheme. This step is called expansion permutation. The result goes through an "exclusive or" (XOR) operation with a transformation of the key K_i with the secret key K shared only by Alice and Bob. The result of this operation is 48 bits long. Putting the result through the "S boxes" returns a 32 bit result. Each of the eight "S boxes" replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The "S boxes" provide the core of the security of DES as without them, the cipher would be linear, and trivially breakable. A last series of permutations that occur in a fixed pattern in the "P boxes" complete the 'f' function.

The only element that remains secret to guarantee confidentiality is the key K. This key is of length 64 bits, with 8 parity bits, for an effective length of 56 bits. The deciphering is done with the inverse diagram and a key inversion. This type of encryption is said to be a "symmetric key" scheme, since the same key serves for encryption and decryption.

The algorithm in itself is not complicated and only employs operations that are binary logic operations or bit permutations. Even with this apparent simplicity, a high level of complexity is achieved, limiting the speed of the DES encryption. For example, a workstation using a HyperSparc processor can encrypt 32000 blocks per second or 2 Mb/s. Some specialized chips reach high speeds. Most encrypt at speeds between 2 and 60 Mb/s [34].

The DES confidentiality limits are well known. A device costing less than a million dollars can implement an exhaustive attack and find the key in three and a half hours [96]. Even if these means are not available to just anybody, we cannot consider DES a very secure encryption technique. Yet, the DES technique of symmetric key encryption was retained for the International Data Encryption Algorithm (IDEA) that is part of the PGP software.

4.1.1.2 RSA

The concept of public key - private key cryptography was invented by Whitfield Diffie and Martin Hellman. The encryption is done using two keys: Alice's private key and Bob's

public key. The combination of these two keys forms a unique key for the communication [24]. RSA was the first algorithm to implement this double key for ciphering and deciphering [81].

The principle of RSA is a mix of simplicity and complexity, with a touch of elegance. The security of the algorithm is based on the extreme difficulty of factoring large numbers. The keys, public and private, are a function of two prime numbers of a least a hundred digits.

To generate a key pair, we choose randomly two large prime numbers, p and q. For the highest security, p and q should be of equal length. The product pq is called n. The encryption key, e, is such that e and $(p-1)(q-1)$ are pairwise prime. The decryption key, d, is defined as $ed \equiv 1 \mod [(p-1)(q-1)]$. The key d is then computed using the formula: $d = e^{-1} \mod [(p-1)(q-1)]$. The two numbers e and n form the public key and d is the private key. Therefore, to encrypt a message m, we just need to divide it into blocks shorter than n and to apply the formula:

$$c_i = m_i^e \mod n, \tag{32}$$

where m_i represents the blocks of cleartext and c_i the blocks of cyphertext.

The decryption is done by applying the "inverse" formula:

$$m_i = c_i^d \mod n. \tag{33}$$

The main RSA limitation is speed. Various implementations on specialized chips are generally one thousand times slower than for a DES encryption. Oddly enough, software implementations of RSA are "only" one hundred times slower than DES [83].

On the other hand, the security of RSA is strong enough that French and Australian banks have made it their encryption standard [27]. Therefore, RSA is a slow cryptographic process but with a confidentiality still recognized.

4.1.1.3 PGP

Pretty Good Privacy is the first powerful cryptographic software that is commercially available and interfaces easily with common electronic messaging software. This software package implements an IDEA-type technique, meaning an algorithm combining multiple rounds of elementary binary operations such as XOR and bit substitutions, for the information encryption and RSA for key distribution. This combination of the two protocols solves the problem of having, within a single program, key distribution and message encryption/decryption. Therefore, PGP operates with two different speeds: low speed (RSA) for the key distribution and high speed (IDEA) for the cypher aspects [104].

The originality of this software is the approach to user authentication. Each user has a pair of keys: a private key and a public key. The private key is secret and stored by each user. On the other hand, the public key is distributed by key servers. PGP proposes a method of showing confidence levels with respect to the authenticity of a public key. Each user can sign public keys and guarantees each key he signs. Little by little, he establishes a key-ring of trust. This system is not flawless but proposes an original solution to the problem of key distribution [83, 104].

4.1.2 System approach

Other techniques are being developed to complement encryption algorithms. These novel approaches base their security on physical principals instead of mathematical algorithms. The two major techniques are chaos cryptography and quantum cryptography. In the following sections, we develop the principal of quantum cryptography before developing our application area within chaos cryptography.

4.1.2.1 Quantum cryptography principle

Quantum cryptography is used to transmit securely an encryption key. The appropriate term for this transmission is quantum key distribution (QKD). With this method, a message is not transmitted, but the secret key needed to encrypt the message is. QKD is a solution

to the fundamental problem of secret key cryptography: key distribution. The alternative of employing a messenger to transport the key is costly in terms of both time and money.

QKD can make use of photon polarization states to encode the ‘0’ and ‘1’ of a key to be shared. Polarization projectors isolate each polarization. Each state can then be detected using a basis formed by orthogonal axes. The basis formed by a vertical and a horizontal projector is frequently used, along with the basis formed by projectors angled at $\pi/4$ and $-\pi/4$. Detecting the incoming photon with the same basis as used at the emitter for the encoding allows for a good measurement. Any measurement done with another basis cannot be certain as to the encoded bit. An experimental implementation uses the bit polarization encoding/decoding protocol with the following five steps, as illustrated in Figure 45.

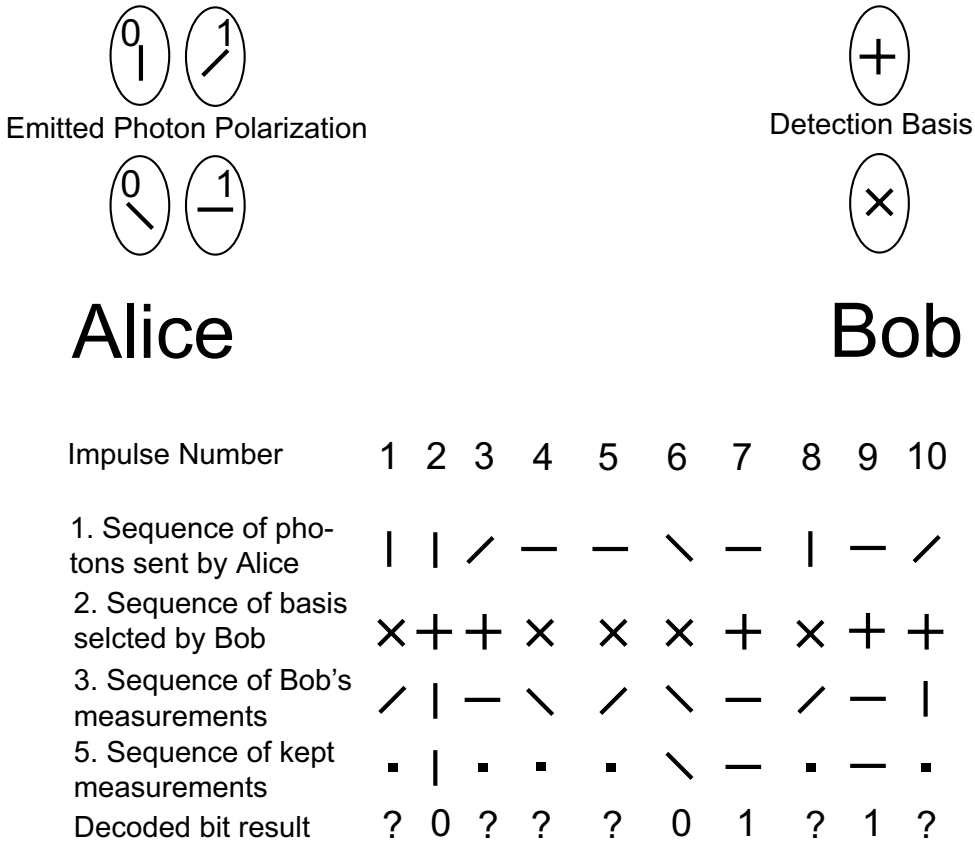


Figure 45: QKD operations diagram.

1. Alice sends a sequence of photons each polarized along one direction (vertical or horizontal, $\pi/4$ or $-\pi/4$).

2. Bob uses a polarization detector. He can angle it to measure vertical, horizontal or 45°polarizations. Each measurement taken with the wrong basis has a random result. Therefore, Bob chooses a random sequence of bases to measure the incident photons.

3. On a public channel, Bob reveals to Alice the series of bases he used for his measurements.

4. Alice informs Bob of basis choices which were good. In our example of Figure 45, the detector was properly set for photons 2, 6, 7, and 9.

5. Bob keeps the properly measured polarizations. By applying a pre-arranged code, Alice and Bob can convert the sequence of polarizations into a key. By having the horizontal and $\pi/4$ polarizations correspond to a '1' bit and the others to a '0' bit, Alice and Bob have the key «0 0 1 1» in our example of Figure 45.

Using this method, Alice and Bob can generate a key of the desired length.

The advantage of this method is that an eavesdropper on the transmission line can be detected. Eve, just like Bob, has to guess the right polarization. And just like Bob, she is going to make mistakes in her choice. Since photons cannot be cloned and observing a photon changes its state, Eve cannot resend an exact duplicated of the photons she observed. Therefore, she introduces additional errors when she eavesdrops. When Alice and Bob compare their results, if Bob has the right polarization basis, yet still detects an error, he will conclude to the presence of a spy on the transmission line [83].

This very strong security is, for the moment, still limited to relatively low bit rates. Current quantum cryptography systems operate at bit rates on the order of tens of kbit/s. Two commercial enterprizes propose QKD products: MagiQ and ID Quantique. Depending on the transmission distance, these systems can generate up to a hundred AES keys of length

256 bits per second. Recent progress by NIST achieved 1 Mbit/s on an aerial transmission of 730 m [13].

4.1.2.2 Quantum cryptography application

If we duplicate the structure of the PGP software, but with systems in mind, quantum cryptography fits in perfectly as the key distribution mechanism: a relatively slow system, functioning in parallel with a fast one. Anticipating a little on Section 4.2.2, the chaotic receiver requires knowledge of a few key parameters to properly decrypt the message. Quantum cryptography is perfectly suited for this role. A complete cryptography system would have QKD complementing the chaos cryptography encryption. We now examine how to decrypt a message transmitted by our chaotic emitter.

4.2 Receiver and system performance

In this section, we detail the study of the receiver starting with the receiver's architecture. This study is completed by examining the synchronization conditions of the receiver to the chaotic oscillations of the emitter. Finally, the complete system, taken as a encryption/decryption method is characterized before integration into a modern telecom network.

4.2.1 Chaotic communication system receiver

The receiver architecture is determined by the emitter architecture, with some slight differences between the two. Before studying in detail the receiver, we summarize the relevant points of the emitter: the system's architecture and the message encoding method.

The emitter must be capable of oscillating chaotically under certain conditions. In our description of the emitter, four functions are regrouped in a closed loop configuration as shown in Figure 23: non-linearity, gain, delay and filtering. The non-linear function is essential for obtaining chaotic dynamics. The linear gain, placed right before this function, enables the signal to sweep multiple extrema of the non-linear function. A least one extrema must be swept to obtain chaotic oscillations. The delay function increases the degrees of freedom for the solutions, as well as the dimension of the phase space. The band

pass filter function takes into account the physical reality of the components we used, as detailed Section 3.2.1.

The message is inserted in this closed loop system (Figure 36) right after the delay function. This technique, inserting the message inside the chaos oscillation loop, is called chaos modulation. The advantages of this method over chaos masking and CSK were presented in Section 3.1.2.

Even though the receiver bears a resemblance to the emitter (i.e. same functional blocks, same components), some aspects are different, and the component layout is done in an open loop architecture (Figure 46). More specifically, the chaotic signal from the transmission is processed via two distinct paths. An optical coupler splits the transmission signal in two. A first coupler output is directly detected by a high-speed photodiode. The electrical signal, which we call the reference signal, thus obtained is proportional by a factor K to the transmitted optical signal. Going back to the terms of Equation (29), the electrical reference signal can be expressed as $K\left[\cos^2(x(t-T)+\phi)+\alpha m(t)\right]$, where K represents the optical coupling factor and the sensitivity of the photoreceiver. The other coupler output traverses the same elements as the emitter feedback signal, starting at the 50/50 coupler (Figure 46). This sequence of components matched to those of the emitter is indicated on Figure 46 by the dashed line box.

The optical signal is detected by a photoreceiver of sensitivity 2 V / mW before being amplified by a wide band linear RF amplifier (30 kHz - 25 GHz) with an 18 dB gain. This amplifier from SHF was specially ordered as a "matched pair" with the emitter amplifier, guaranteeing very close characteristics for the two components. A plot of the S_{21} parameter of each amplifier was given in Figure 30. Similarly, the receiver electro-optic modulator is quite similar to the emitter one, as attested by Figure 33. The insertion losses were measured as 1.8 dB and the half wave voltage V_π as 4.4 V. These characteristics are only slightly different from the emitter modulator, which has insertion losses of 1.6 dB and a half wave voltage of 4.2 V. However, exact characteristic matching is not critical here: the

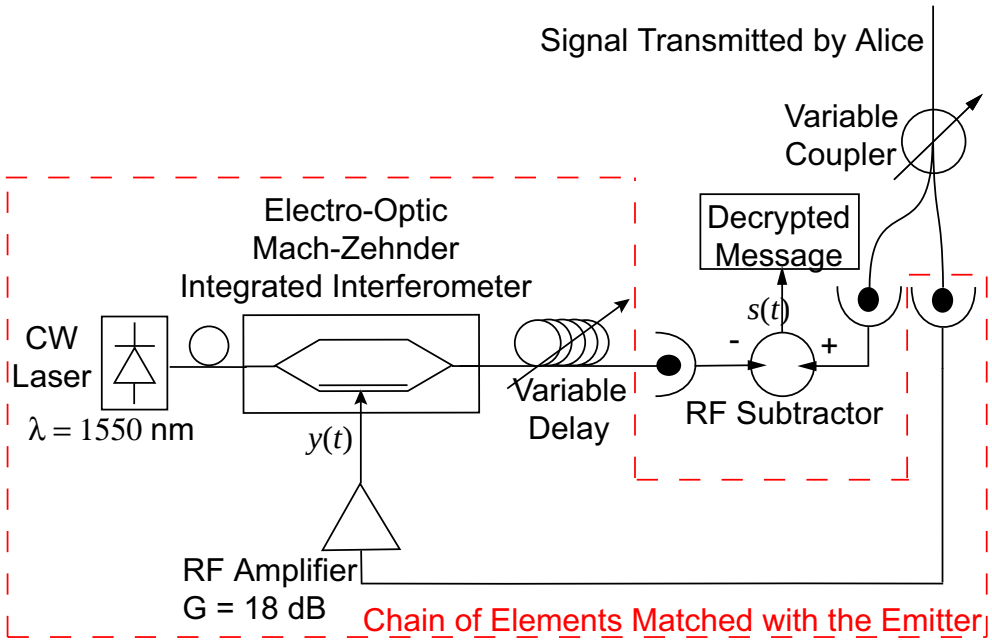


Figure 46: Receiver experimental diagram.

global loop gain can be adjusted by the CW laser output power or by the variable gain of the photoreceiver.

At the output of the delay line, the chaos has been replicated locally at the emitter and can be written as the solution to the following equation:

$$y(t) + \tau' \frac{dy}{dt}(t) + \frac{1}{\theta'} \int_{t_0}^{t} y(\xi)\, d\xi = \beta' \left[\cos^2(x(t-T) + \phi) + \alpha\, m(t) \right]. \tag{34}$$

The apostrophe symbols indicate receiver parameters. The β' parameter is the global gain from the optical coupler and the RF input of the modulator. It multiplies the transmitted signal from Alice: $\cos^2(x(t-T)+\phi) + \alpha\, m(t)$. The optical output of the modulator is delayed before detection. This signal, $K' \cos^2[y(t-T') + \phi']$, will be used in conjunction with the reference signal to recover the message. The gain coefficient K' is a function of the CW laser output power and the sensitivity of the photoreceiver that detects the signal after the modulator and the variable delay line. The phase shift ϕ' corresponds to the normalized bias voltage of the modulator. The addition of the reference signal with the replicated chaos signal is done with a wide band power divider (DC - 26 GHz) used as a power combiner (2

input signals, one output). The output signal $s(t)$ of this power divider is:

$$s(t) = K \cdot \{\cos^2[x(t-T)+\phi] + \alpha m(t)\} + K' \cos^2[y(t-T')+\phi'] \quad (35)$$

When the receiver is perfectly tuned, the signal $s(t)$ is proportional to $m(t)$. Indeed, the addition of the replicated chaos to the reference signal is done in such a way as to cancel the chaotic component of the transmitted signal. To achieve this, the receiver modulator is biased with the appropriate voltage. The ϕ' parameter is adjusted as to have $\cos^2[\phi] = 1 - \cos^2[\phi']$, i.e. $\phi' = \phi \pm \pi/2$. Then, the replicated chaos becomes the negative image of the emitter chaos up to a DC constant. This constant is then filtered out by the band pass process of the photoreceiver. The addition that the power divider performs is in fact the subtraction of the replicated chaos from the reference signal. From this difference, we obtain the decrypted message. This technique only yields good results if the replicated chaotic oscillations match perfectly the emitter oscillation right before the message is optically inserted.

The study of the chaos replication, and, specifically, the exactness of this replication as a function of the different receiver parameters constitutes the decoding key, and, hence, is necessary for the proper functioning of the communication between emitter and authorized receiver.

4.2.2 Synchronization

The study of the synchronization of the receiver to the emitter was done on the system represented in Figure 47.

The objective was to study the similarity between signals X and Y that represent, respectively, the reference signal and the chaos replicated at the receiver. This study was carried out without including any message: only the chaotic carrier is transmitted to the receiver. The carrier's spectrum has been presented in Figure 42, and proper synchronization needs to be achieved over several GHz.

The purpose of the receiver is to reproduce the oscillations of the emitter as exactly

as possible. This process, termed "synchronization," stems from the research of Pecora and Carroll [77]. Other works have already demonstrated the synchronization of chaotic oscillators based on Ikeda cavities [23]. The use of the very general term "synchronization" hides the fact that we are really observing replication. Indeed, the receiver is completely passive (i.e. without input from the emitter, the receiver produces no output).

As a metric to evaluate the synchronization quality, we define the following quantity:

$$e_{dB} = 10 \log_{10}\left(\frac{< X - Y >^2}{< X^2 >}\right), \tag{36}$$

as representing the synchronization error in the time trace. This metric is a measure of the difference between the chaos at the emitter and the replicated one at the receiver. The number of time samples considered make this error measurement local (few samples) or global (many samples). In a telecom framework, we are interested in the global error obtained over long periods of time. Therefore, 10^5 samples were used in these calculations. The error was also characterized in the spectral domain.

A typical example of chaotic time traces, both for the emitter and the receiver is presented in Figure 48 as well as the X-Y plot that gives a rough view of the replication quality. We aim to have an X-Y plot with a line as thin as possible at a 45 angle. This signifies that the X-axis variable is equal to the Y-axis variable. The thickness of the line provides a visual indication of the replication error, hence on its quality.

For the time traces of Figure 48, e_{dB} is computed to be -12 dB. The only problem with this measurement method is that the oscilloscope has a bandwidth of 5 GHz. We have seen in Figure 42 that the signals we are measuring here have a bandwidth of roughly 6 GHz. Other measurement methods were then developed using higher bandwith equipment.

Interrupting the flow a bit, we note that, as explained in Section 4.2.1, the bias voltage of the modulator can be set to obtain an "inverse" replication, where the replicated chaos is exactly the opposite of the emitter chaos. This process is illustrated experimentally in Figure 49. We principally make use of the inverse synchronization, since the power divider set up as a combiner performs an addition of the electrical input signals.

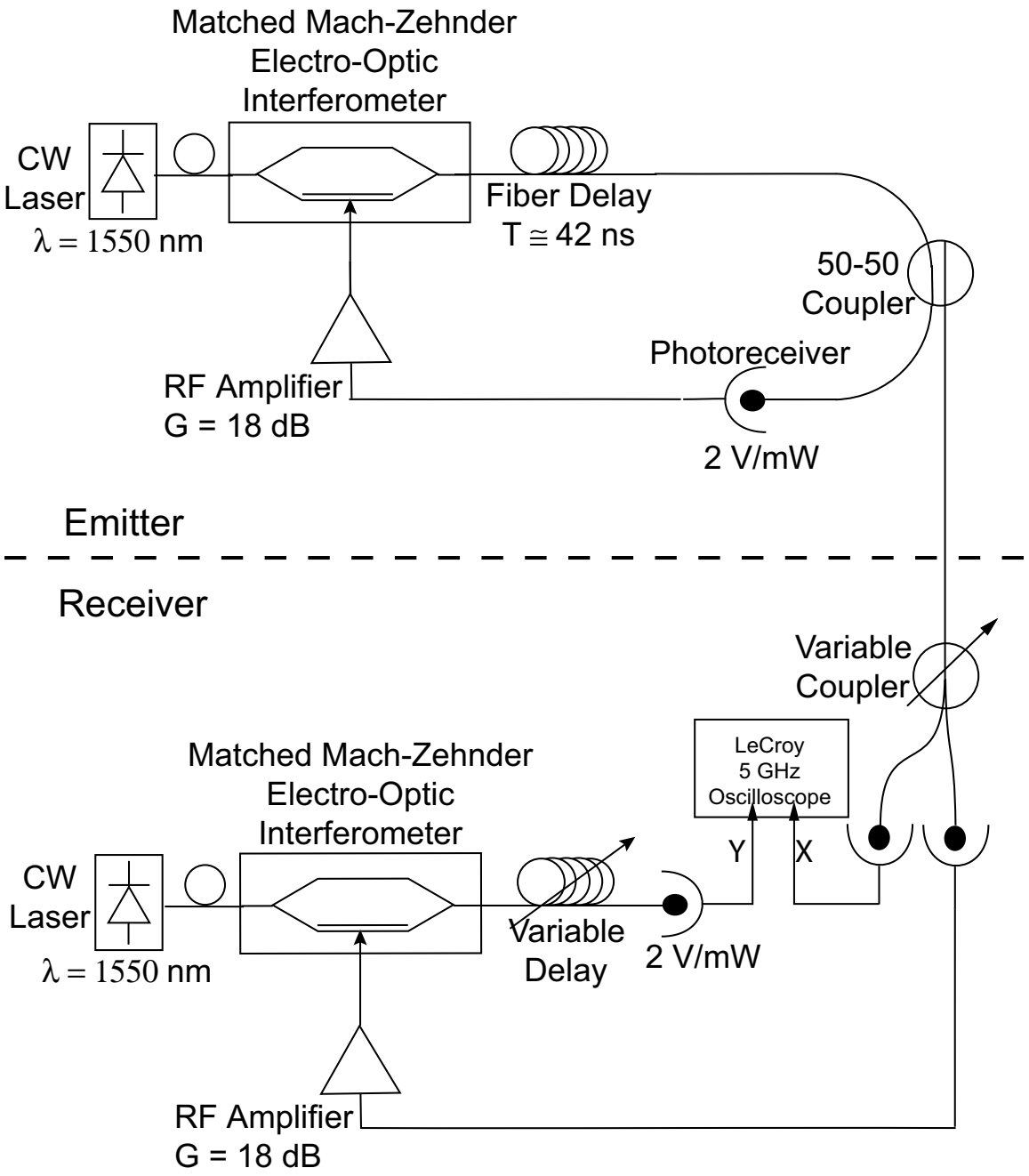


Figure 47: Synchronization evaluation experimental setup.

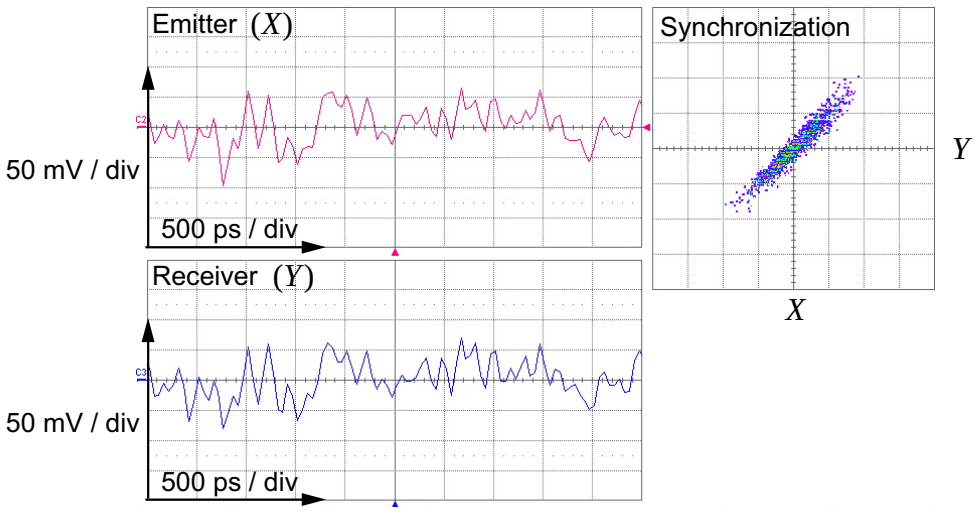


Figure 48: Typical example of synchronized time traces, $Y = X$.

Returning to the error measurements, another method consists in comparing spectrally the levels of chaos and the decoding noise without any message. By connecting an RF spectrum analyzer on the output signal of Figure 50, the spectral evolution of the error signal, also called "decoding noise" can be visualized in real time. This method helps in properly adjusting the receiver parameters. With the emitter oscillating in the chaotic regime, we adjust the receiver parameters so the output signal (Figure 50) presents a spectrum as low and as flat as possible.

The synchronization quality as a function of the different receiver parameters was the focus of an analytical, numerical, and experimental study done in partnership with the *Instituto Mediterraneo de Estudios Avanzados* (IMEDEA) of the *Universitat de les Isles Baleares*. Only the effects of the three parameters experimentally controllable will be presented in this chapter. These parameters are the bifurcation parameter β, the delay T, and the phase ϕ [16].

The system can be modeled by two equations, one for the emitter, and one for the

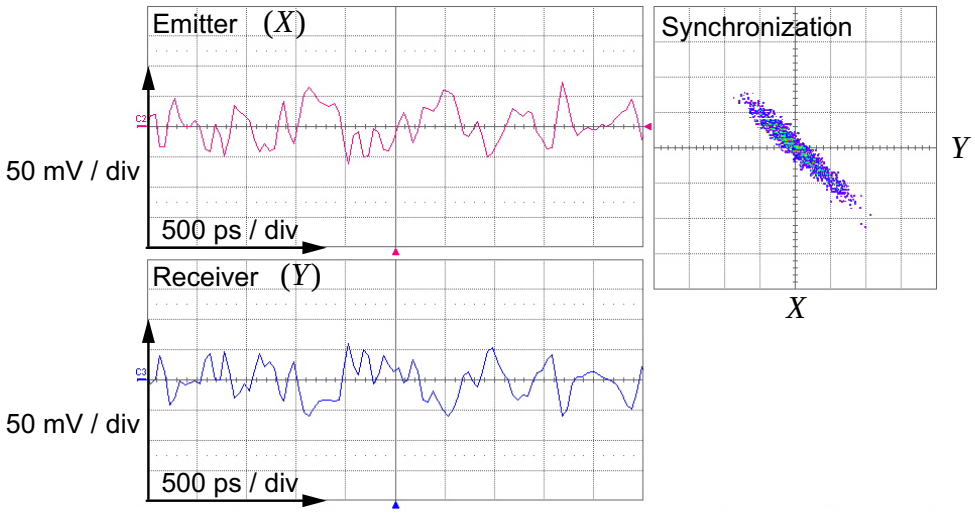


Figure 49: Inverse synchronization, $Y = -X$.

receiver:

$$x + \tau\frac{dx}{dt} + \frac{1}{\theta}\int_{t_0}^{t} x(s)\,ds = \beta\cos^2[x(t-T)+\phi] \tag{37}$$

$$y + \tau'\frac{dy}{dt} + \frac{1}{\theta'}\int_{t_0}^{t} y(s)\,ds = \beta'\cos^2[x(t-T')+\phi'] \tag{38}$$

In these equations, the message term $m(t)$ was omitted as we are only examining synchronization to the chaotic carrier. The original experimental system diagram is found in reference [16].

The first step consists of a variable substitution in Equation (37) to introduce the variable $u(t)$:

$$u(t) = \int_{t_0}^{t} x(s)\,ds. \tag{39}$$

Equation (37) then becomes an ordinary, second-order linear differential equation:

$$\dot{u} + \tau\ddot{u} + \frac{1}{\theta}u = \beta\cos^2[x(t-T)+\phi]. \tag{40}$$

Considering the wide bandwidth of the system and the roots of the characteristic polynomial corresponding to the homogeneous solution of (40), the stationary solution for u can be formally expressed as:

$$u(t) = \beta\int_{t_0}^{t}\left[e^{\frac{s-t}{\theta}} - e^{\frac{s-t}{\tau}}\right]\cos^2[x(s-T)+\phi]\,ds. \tag{41}$$

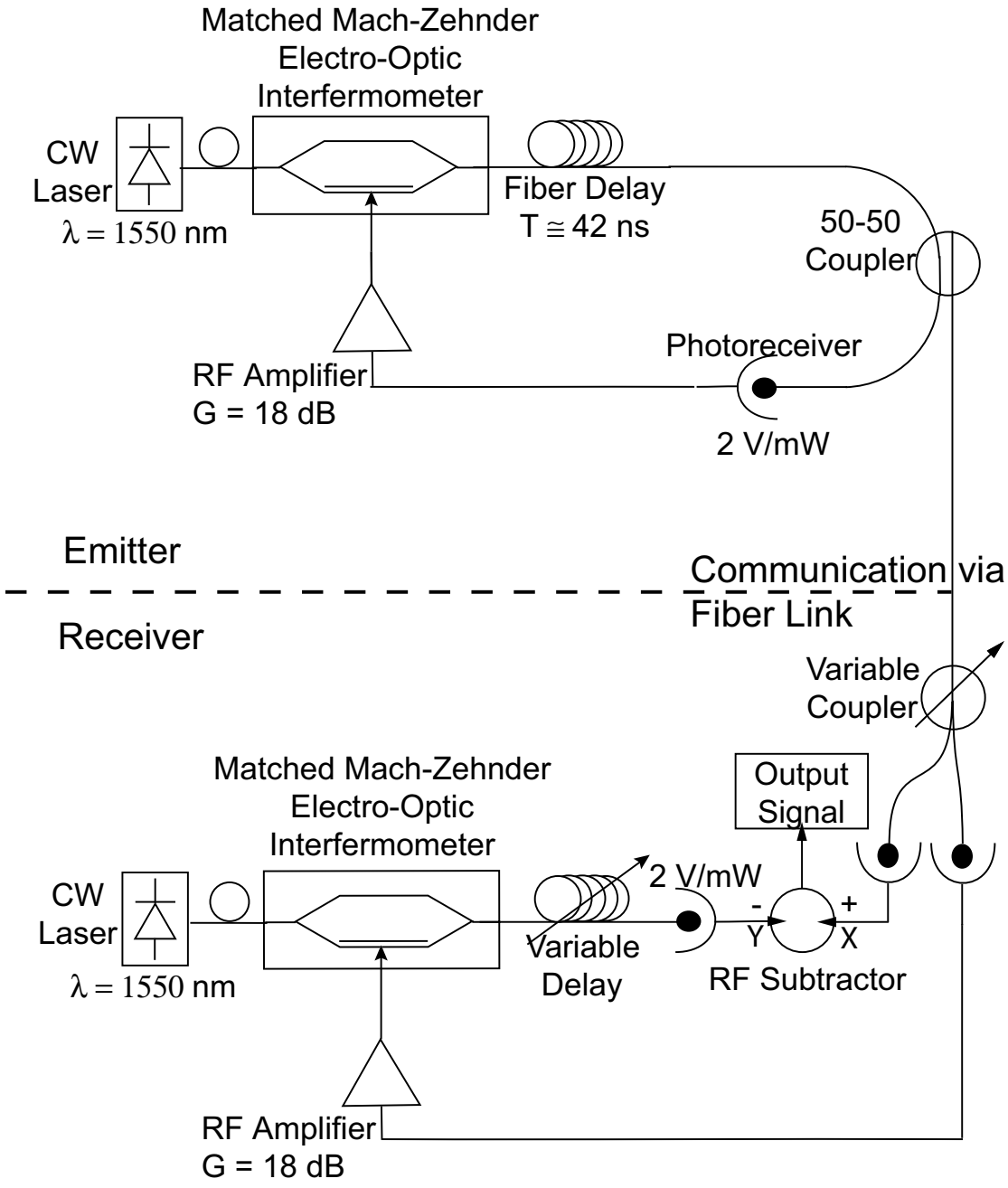


Figure 50: Experimental synchronization observation diagram.

Then, $x(t)$ can be expressed as:

$$\begin{aligned} x(t) &= \beta \int_{t_0}^{t} U(s,t) \cos^2[x(s-T)+\phi]\, ds, \\ U(s,t) &= \left(\frac{1}{\tau} e^{\frac{s-t}{\tau}} - \frac{1}{\theta} e^{\frac{s-t}{\theta}}\right). \end{aligned} \tag{42}$$

$U(s,t)$ is only a function of the system filter parameters. By proceeding in a similar fashion, we reach a parallel expression for $y(t)$ at the receiver:

$$y(t) = \beta' \int_{t_0}^{t} U'(s,t) \cos^2[x(s-T')+\phi']ds. \tag{43}$$

With Equations (42) and (43), we can define the metrics for measuring synchronization quantity. We define for each parameter p the instantaneous synchronization error as:

$$\epsilon_{\Delta p}(t) = y_{p'}(t) - x_p(t). \tag{44}$$

The normalized instantaneous error of which we take the RMS value is defined as:

$$\sigma_{\Delta p} = \sqrt{\frac{< \epsilon_{\Delta p}^2 >}{< x_p^2 >}}. \tag{45}$$

The value $\sigma_{\Delta p}$ represents a time averaged error relative to the proximity of the emitter and the receiver time traces. When using this average, we must integrate over a time longer than the longest system time period, determined by the lower cutoff frequency θ, to consider all the frequencies present in the error signal.

After these preparatory steps, we are ready to study the synchronization error as a function of the individual parameter mismatches.

4.2.2.1 Bifurcation parameter β mismatch

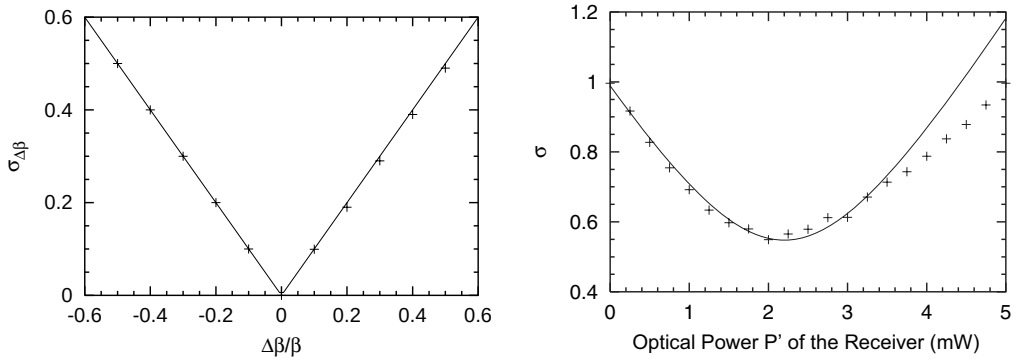
We start our study with the bifurcation parameter β. This parameter corresponds to the normalized gain of the opto-electronic feedback loop. Physically, β is function of the electro-optic sensitivity of the modulator (V_π), of the conversion factor of the photoreceivers, of the optical losses (coupling, insertion) and of the CW laser optical output power P. Individual variations of these values are of no consequence, so long as the resulting value for β is not

affected. For example, different optical losses can be compensated for by adjusting the CW laser output power. We make the hypothesis that all the other parameters (except β) are perfectly matched. Therefore, $\phi' = \phi$, $\tau' = \tau$, $\theta' = \theta$ and $T' = T$.

By combining Equations (42) and (43), we find $x(t) = \beta y(t)/\beta'$. Therefore $\epsilon(t) = (\Delta\beta/\beta)x(t)$ with $\Delta\beta = \beta' - \beta$. Hence, the average synchronization error can be expressed as:

$$\sigma_{\Delta\beta} = \left|\frac{\Delta\beta}{\beta}\right| \tag{46}$$

The synchronization error is therefore directly proportional to a bifurcation parameter mismatch.



(a) Analytical (–) and numerical (+) study. (b) Analytical (–) and experimental study (+).

Figure 51: Synchronization error as a function of the β parameter computed analytically and numerically, then measured experimentally.

Figure 51 presents the result of the β mismatch study. Firstly, Figure 51(a) compares the analytical study to the numerical results from Equations (42) and (43). These results validate Equation (46). The absolute value in Equation (46) is responsible for the symmetry of Figure 51(a). Experimentally, plots with a sharp vertex are much harder to obtain because some residual mismatch always remains in the other parameters, although these mismatches were considered zero by hypothesis. Thus, the notation of the synchronization error is slightly different between Figures 51(a) and 51(b). The residual mismatch in the other parameters precludes the use of Equation (46) when comparing experimental and analytical plots. Therefore, another, more general, error formula was proposed: Equation

(69) of [16]:

$$\sigma = \sqrt{\sum_{i,j=1}^{5} M_{ij} z_i z_j} = \sqrt{\mathbf{z^T M z}}. \tag{47}$$

The variable $\mathbf{z}$ is the vector $(\Delta/\tau, \Delta\beta/\beta, \Delta\phi, \Delta\theta/\theta, \Delta\tau/\tau)$ and $\mathbf{M}$ represents the symmetric characteristic matrix of the quadratic form. The solid line curve of Figure 51(b) represents the synchronization error adjusted for the residual error on the parameters other than β. This residual mismatch explains the rounded shape of the plot in Figure 51(b). Yet, the slopes of the experimental plot are not the same on each side of the optimal point. We observe on the right side of the plot (when $P' > P$) a smaller slope than on the left side. We are probably seeing the effects of saturation on the linear gain elements when the optical power gets too high.

Finally, we point out the direct proportionality linking optical power to gain β as given by Equation (30e). Therefore, we can equate $\Delta\beta/\beta$ and $\Delta P/P$.

4.2.2.2 T Delay mismatch

To study the influence of the T' delay mismatch on synchronization quality, we again make the hypotheses that all the other parameters are perfectly matched. Hence, we have $\beta' = \beta$, $\phi' = \phi$, $\tau' = \tau$ and $\theta' = \theta$. We set $\Delta T = T' - T$. With these hypothesis, we rewrite Equation (43):

$$\begin{aligned} y(t) &= \beta \int_{t_0}^{t} U(s,t) \cos^2[x(s - T - \Delta T) + \phi]\, ds \\ y(t) &= x(t - \Delta T) + \beta \int_{t_0 - \Delta T}^{t_0} U(s', t - \Delta T) \cos^2[x(s' - T) + \phi]\, ds' \end{aligned} \tag{48}$$

with $s' = s - \Delta T$. The second integral term decreases exponentially and becomes negligible in steady state. Therefore, we have:

$$y(t) = x(t - \Delta T). \tag{49}$$

As indicated in Equation (49), a delay mismatch at the receiver influences the chaos replication by creating a time shift of the value of the mismatch. The receiver's chaotic dynamic has not been modified.

Because of the high speed of the chaotic fluctuations with respect to the delay, which is much greater than τ, we can expect a small mismatch to introduce a high synchronization degradation.

We take $X(\omega)$ as the Fourier transform of $x(t)$. We note that this is a slightly different definition of the Fourier transform then given in Equation (11) as it uses the pulsation ω instead of frequency f. Equation (49) gives us $Y(\omega)$, the Fourier transform of $y(t)$, as: $Y(\omega) = e^{-i\omega\Delta T}X(\omega)$. The synchronization error defined by (45) becomes:

$$E(\omega) = \left[e^{-i\omega\Delta T} - 1\right] X(\omega) = H_T(\omega)X(\omega) \tag{50}$$

with $H_T(\omega)$ the transfer function from $E(\omega)$ to $X(\omega)$ for a ΔT mismatch. The synchronization error can be expressed theoretically using Parseval's theorem as:

$$\sigma^2_{\Delta T} = \frac{\int_{-\infty}^{+\infty} |H_T(\omega)|^2 \, |X(\omega)|^2 \, d\omega}{\int_{-\infty}^{+\infty} |X(\omega)|^2 \, d\omega} \tag{51}$$

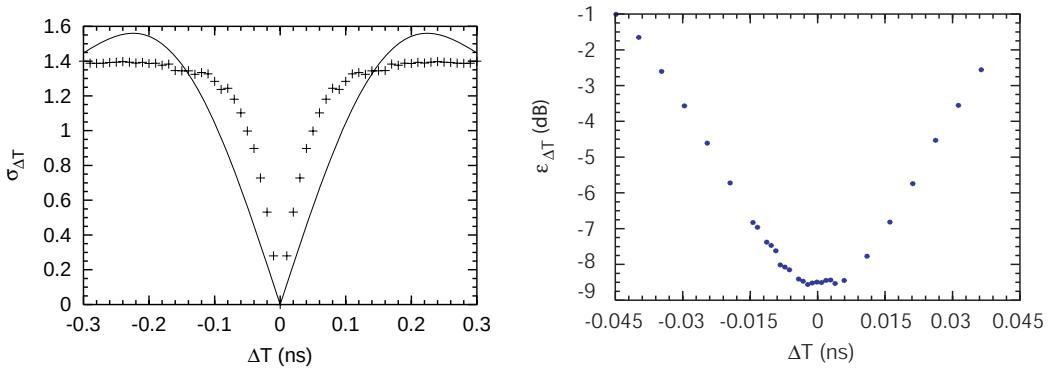
The integrals of (51) are not computable analytically. As a first approximation, we can consider that $X(\omega)$ has a spectral signature close to a rectangle with the limits of the band pass filter. Therefore,

$$X(\omega) = \begin{cases} S \text{ if } \omega \in \left[-\frac{1}{\tau}, -\frac{1}{\theta}\right] \cup \left[\frac{1}{\tau}, \frac{1}{\theta}\right] \\ 0 \text{ otherwise} \end{cases} \tag{52}$$

In Equation (52), S is a non-zero arbitrary real number whose value is of little importance since the synchronization error is normalized with the amplitude of the chaotic signal. We can deduce:

$$\begin{aligned} \sigma^2_{\Delta T} &\approx \frac{1}{\tau^{-1} - \theta^{-1}} \int_{1/\theta}^{1/\tau} |H_T(\omega)|^2 \, d\omega \\ &\approx 2\left[1 - \text{sinc}\left(\frac{\Delta T}{\tau}\right)\right]. \end{aligned} \tag{53}$$

Equation (53) is an analytical form of the synchronization error as a function of delay mismatch ΔT. This mismatch is also computed numerically and evaluated analytically in Figure 52.



(a) Analytical (–) and numerical (+) study.

(b) Experimental study.

Figure 52: Synchronization error as a function of delay mismatch ΔT computed analytically, numerically, and measured experimentally.

The analysis and the numerical calculations give similar results, yet are not superimposed for all mismatches (Figure 52(a)). Yet the two plots present the same general aspect: two plateaus of poor synchronization with a 'V' shaped dip and a sharp vertex of high synchronization. We can compare the width at half-height of the analytical and numerical plots to be, respectively, 0.12 and 0.6 ns. For a synchronization loss of 6 dB, the width of the plots are then 0.32 and 0.34 ns, the numerical plot being narrower than the analytical one.

A first experimental study was conducted with equipment unable to precisely measure the variations of the time delay. Note that the receiver properly synchronizes with the emitter, but not at the right moment. We observe a time shift of the receiver time trace, even if the signal retains the same variations as the emitter [16].

With the purchase of the motorized fiber delay line from General Photonics, a more precise experimental study was undertaken (Figure 52(b)). This delay mismatch study was done over a much smaller set of values than for the numerical study: we limited ourselves to variations of ±45 ns from the correct delay value. The Y-axis of Figure 52(b) is now a logarithmic scale to highlight the synchronization quality changes as a function of delay mismatch. We preferred to plot the synchronization error as defined by Equation (36). We can then notice synchronization variation for delay mismatches as small as 2 or 3 ps.

Quantitatively, the width of the curve, 3 dB above the minimum synchronization point (at the −6 dB level) is 0.3 ns. The value is to be compared with the 0.12 and 0.06 ns for the analytical and numerical plots.

As we had noticed for the gain mismatch (Figure 51(b)), a residual parameter mismatch explains the flattening out and the lack of sharp vertex on Figure 52(b), at $\Delta T = 0$.

4.2.2.3 Phase ϕ mismatch

A phase mismatch is often caused by a residual optical path difference in the modulators. This difference can be compensated experimentally by a DC bias voltage applied to the DC electrodes of the modulators.

To study the effect of the ϕ parameter mismatch, we rewrite Equation (42) as:

$$x(t) = \frac{\beta}{2}\int_{t_0}^{t} U(s,t)\,ds + \frac{\beta}{2}\int_{t_0}^{t} U(s,t)\cos[2x(s-T)+2\phi]\,ds. \tag{54}$$

The first term of the right hand side decreases to 0 when t increases as the result of the DC component filtering. We can then examine the stationary solutions for $x(t)$ and $y(t)$ as:

$$\begin{aligned} x(t) &= \frac{\beta}{2}\int_{t_0}^{t} U(s,t)\cos[2x(s-T)+2\phi]\,ds, \\ y(t) &= \frac{\beta}{2}\int_{t_0}^{t} U'(s,t)\cos[2x(s-T')+2\phi']\,ds. \end{aligned} \tag{55}$$

To simplify the expression, we set:

$$Q(s,t,\phi) = U(s,t)\cos[2x(s-T)+2\phi]. \tag{56}$$

If we make the hypothesis that $\beta' = \beta$, $\theta' = \theta$, $\tau' = \tau$, $T' = T$ and $\Delta\phi = \phi' - \phi$, the instantaneous synchronization error is expressed by:

$$\epsilon(t) = -\beta\sin(\Delta\phi)\int_{t_0}^{t} Q\left(s,t,\phi+\frac{\Delta\phi}{2}-\frac{\pi}{4}\right)ds. \tag{57}$$

Previous works have demonstrated that phase has little influence on the global (average) properties of the chaotic dynamic, if the delay T and the bifurcation parameter β are big enough. These results were obtained numerically by the computation of the Lyapunov

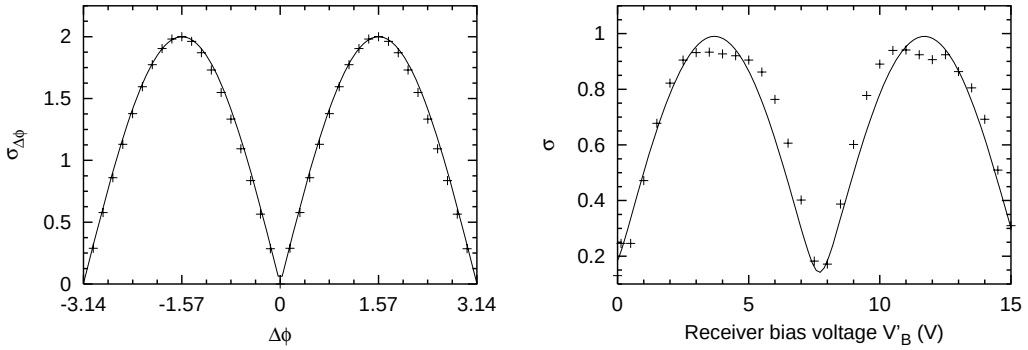
exponents [25]. Other investigations concluded that, under the same conditions, the number and the values of the positive Lyapunov exponents are hardly dependent on the phase parameter [93, 94]. The Lyapunov exponents were computed for various values of β and ϕ from Equation (19).

From Equation (57), with this hypothesis, and taking the error average, we obtain the quadratic error:

$$\begin{aligned} \left\langle \epsilon^2_{\Delta\phi} \right\rangle &\approx \beta^2 \sin^2(\Delta\phi) \left\langle \left[\int_{t_0}^{t} Q(s,t,\phi)\, ds \right]^2 \right\rangle \\ &= 4 \sin^2(\Delta\phi) \left\langle x^2 \right\rangle . \end{aligned} \tag{58}$$

The standard deviation for a phase mismatch is then defined by:

$$\sigma_{\Delta\phi} = 2\,|\sin(\Delta\phi)|\,. \tag{59}$$



(a) Analytical (–) and numerical (+) study. (b) Analytical (–) and experimental study (+).

Figure 53: Synchronization error as a function of the phase ϕ parameter computed analytically, numerically, and measured experimentally.

The approximations that were done during the calculations that lead to Equation (59) are a posteriori justified by the close fit between analytical and numerical plots in Figure 53(a). The experimental and numerical plots also show a good match between the experimental and the numerical results (Figure 53(b)).

4.2.3 An encrypted communication system

Previously, in Section 4.2.1, we studied the receiver's architecture and synchronization quality. We now propose to establish the link between synchronization quality and the

future use of this system in optical communication. To quantify the quality of a communication link, the usual metric is the Bit Error Ratio (BER). The BER is the ratio of the number of decoding errors to the number of bits sent through the communication system. An acceptable BER value for a modern telecom link in 10^{-9}, that is, one error for every billion bits that go through the communication system. The synchronization quality directly influences the communication quality, as quantified by the BER. The previous study enables us to be in optimal communication conditions for performing the best possible measurements of the BER.

The device that performs the BER measurement is a Digital Signal Analyzer (also called a BER Tester) and is composed of three main parts. The first one is a frequency synthesizer that generates a clock signal at the desired message frequency. The second part is the Pulse Pattern Generator (PPG). This device uses the clock signal from the synthesizer to generate a pseudo-random bit sequence (PRBS) at the desired frequency, which serves as the message to test the system communication quality. The third part of the Digital Signal Analyzer of the error detector (ED) that detects and counts the errors after transmission. By comparing the detected signal to a set threshold level, the error detector decides if the incoming bit is a '0' or a '1'. After comparing with the signal emitted from the PPG, the bit is counted as correctly decoded or as an error. The BER is therefore computed by sending long pseudo-random bit sequences to be transmitted and decoded [85].

Experimentally, we use a PRBS of length $2^7 - 1$ (127) bits as message. This message is inserted into the chaotic emitter by direct modulation of a laser diode with an electrical signal corresponding to the PRBS. A variable optical attenuator controls the optical power of the message allowing for the adjustment of the factor α present in Equations (29) and (34).

The decoded message is analyzed by the Digital Signal Analyzer to measure the BER in the setup described by Figure 54. Hence, by varying the masking factor α at the emitter, we vary the amplitude difference of the "high" and "low" levels of the message relative to the RMS fluctuations of the chaotic carrier which are constant for a given choice of values

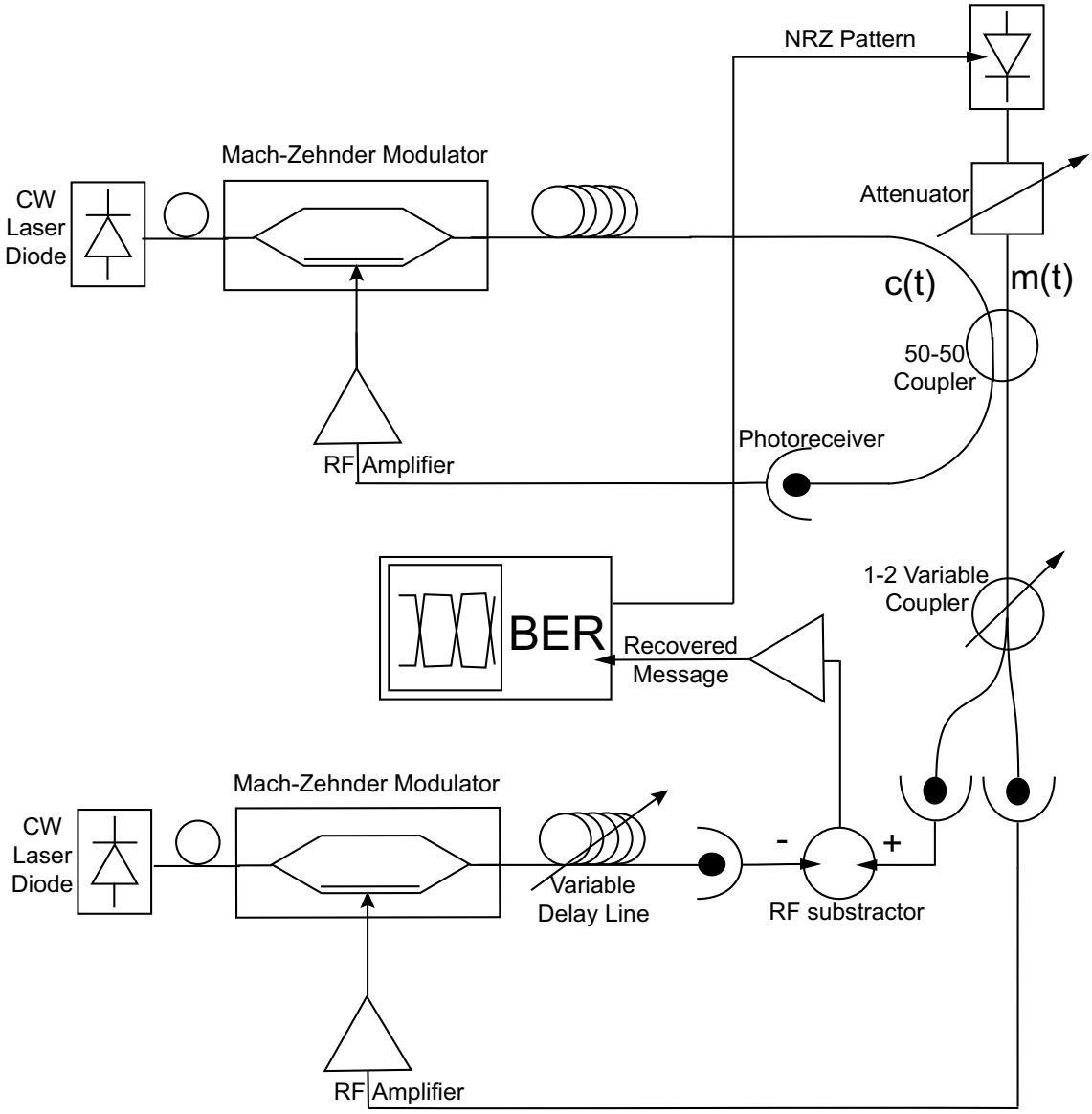


Figure 54: Experimental diagram of BER measurement.

for the chaos generation parameters. A wider gap allows for a better differentiation of ‘0’ and ‘1’, reducing decoding errors. The tradeoff is that the message is bigger relative to the chaotic carrier amplitude and, thus, is less masked during transmission.

Depending on the variations of α, we observe variations of the BER with constant synchronization quality. The BER is represented as a function of α in Figure 55. The two lines on the plot represent the BER associated with an authorized receiver (BER BOB) and with direct listening on the transmission line as a spy would do (BER EVE). For the communication system to be secure, a spy should not be able to extract any information from the transmitted signal. Therefore, the message masking factor α is adjusted so the message cannot be detected by Eve inside the chaotic transmission. The chaotic carrier acts similarly to noise inside which the message is hidden. The objective is to maximize the information Bob receives while minimizing (to zero) the information Eve collects. The vertical separation in Figure 55 symbolizes this difference in the information quantity the two competitors (Bob and Eve) obtain from the transmitted signal. We can also view the chaotic carrier as noise for the message. The receiver behaves as a filtering element that rejects the chaotic "noise." The higher the synchronization quality, the more the chaotic carrier will be filtered out of the transmitted signal. Transposed in a cryptographic context, the previous principle relates decoding quality to confidentiality. A chaotic noise rendered very low by a properly tuned receiver allows for a reduction of the message power (by reducing α). Therefore, the message is more efficiently masked in the transmission line.

Defining the confidentiality level of a transmission is not easy. How do we determine if a transmission is secure or not? One answer to this question, for the system under study, is twofold as there are two possible approaches to attack this system. The first attack consists in deciphering "on the fly" the message, in real-time, directly as the signal is transmitted. We discuss system security against this eavesdropping technique further along in this chapter. The second approach consists of recording the transmitted signal and proceeding to attack the code at a later moment. Within this second general method, the techniques are

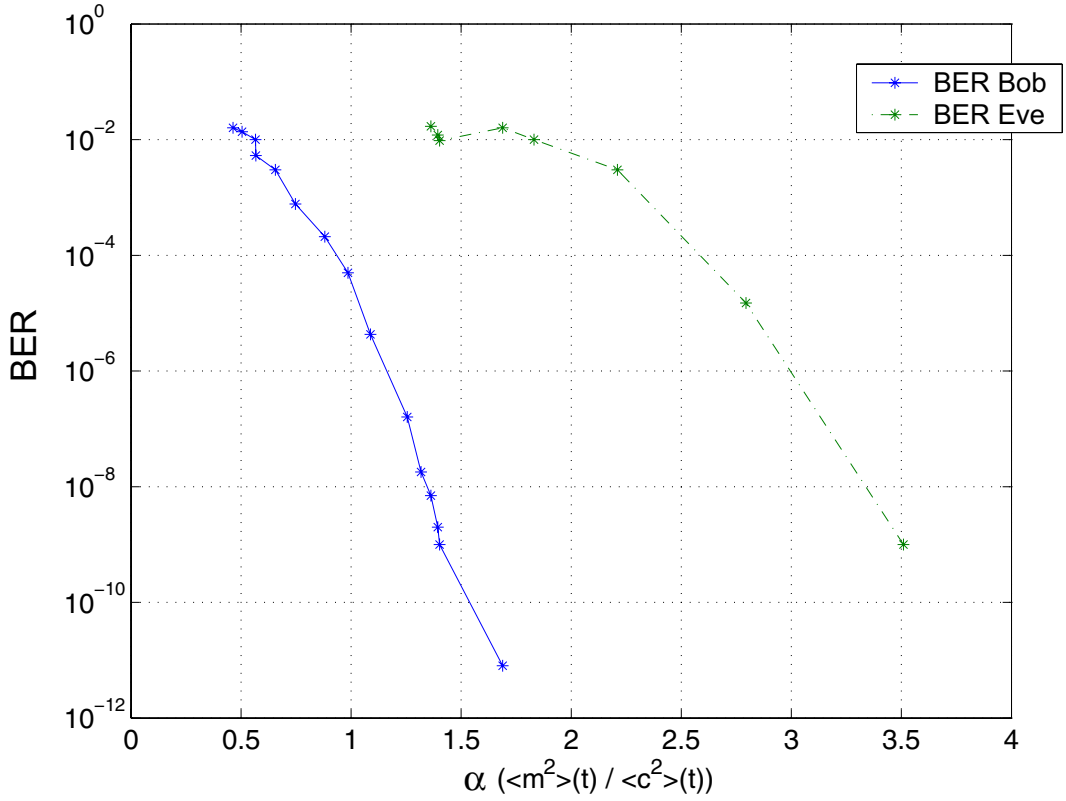


Figure 55: Comparative plot of the BER with a 3 GHz message for Bob and Eve as a function of the masking factor α.

numerous. We will detail some aspects of this "deferred" cryptanalysis in the next chapter (Section 5.1.3).

Going back to the analogy between the chaotic carrier and noise, for a non-authorized receiver, the chaos appears as noise on the transmission line. This chaos, as any noise would, impedes the communication. When the chaos induced perturbation is big enough, direct detection does not yield a reliable decision on the transmitted bit. A spy is then faced with the same probability for a '1' bit as for a '0' bit, independent of the bit value that was encoded. The message is then properly encrypted, since Eve cannot differentiate bits decoded properly from the errors. This condition gives us a first approach for "on the fly" cryptanalysis and for the meaning of security.

We now need to transform this security condition into a practical constraint. The error detector of the digital signal analyzer is incapable of measuring a BER greater than 10^{-2}

in the sequences the analyzer receives. Note that this module receives clock information from the PPG, which includes the message frequency and the beginning of each new bit. Without this information, the ED is completely unable to measure a BER. An eavesdropper would not have access to this clock information, which complicates message hacking.

The transmitted signal is analyzed directly by the error detector without the receiver. In this case, the ED plays the role of Eve trying to decode the signal. Therefore, when the ED cannot measure a BER, we consider the message to be efficiently masked. This threshold is reached when the ED cannot establish its decision making criteria determined by the time offset (with reference to the clock) and the threshold separating a '1' from a '0' [85]. When the ED cannot set these parameters, we consider the '1' and '0' levels not sufficiently distinguishable for the device, the masking effective and the communication secure. Yet, when the masking is insufficient (i.e. α is too big), the ED differentiates reliably the two levels and extracts at least parts of the message. The error rate of a non-authorized receiver is plotted in Figure 55. The plot "BER Eve" starts at $\alpha = 1.3$ because, when the masking is more significant (and α is smaller), the BER cannot be measured.

This limit of $\alpha = 1.3$ in Figure 55 constitutes the limit of Eve's ability to decode the message. A visual measure is obtained by constructing the eye diagram. This visualization provides a less abstract grasp of the decoding problem. To construct the eye diagram, a wideband oscilloscope is triggered by the message clock signal. Multiple time traces can be superimposed on the oscilloscope screen. The eye opening gives a visual appreciation of the decoding quality.

Figure 56 shows the decoded signal eye diagram with a BER measured at $7 \cdot 10^{-9}$ for $\alpha = 1.3$. This figure shows three bit periods. By using the oscilloscope remanence, multiple traces are displayed on the screen. The color codes for the number of times the time trace has passed by a specific point. The color map starts with a dark purple for a low count to bright red for a high count. On Figure 56, the black space that constitutes the eye opening is the feature of significance. The more the eye is open, the better differentiated the high

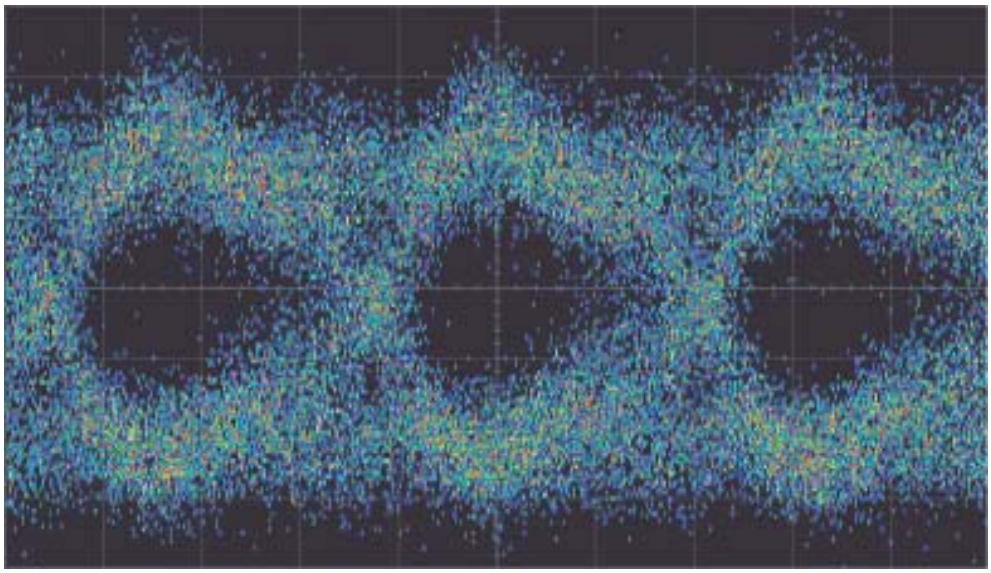


Figure 56: Bob's eye diagram.

and low levels are, and the better the decoding is. Another factor contributes to the eye opening: the transition time between levels, linked to the system response time.

To visually evaluate the masking efficiency, the eye diagram was constructed for Eve, after direct detection of the transmitted signal, without the receiver decoding. Figure 57 presents a series of bits, as seen by Eve for the same value of $\alpha = 1.3$. A quick comparison of Figures 56 and 57 shows the difficulty Eve has in detecting properly a signal, contrasting with the ease Bob has. In Figure 57, the error detector measures with difficulty a BER of $1.6 \cdot 10^{-2}$. Remember that the ED receives clock information from the PPG to trigger on. An authentic spy on the line would not have this access. Before any decryption attempt, an unauthorized receiver needs to determine the message frequency to separate bits and trigger the bit decision ('0' or '1').

With a direct detection of the transmission line, a spy can also perform a spectral analysis of the signal to gain information on the message. We, therefore, compare the spectrum of the message with that of the transmission signal (Figure 58).

We recall that the message is Non Return to Zero (NRZ) encoded PRBS of 127 bits. The spectral signature of this type of signal is a function with a zero at the clock frequency

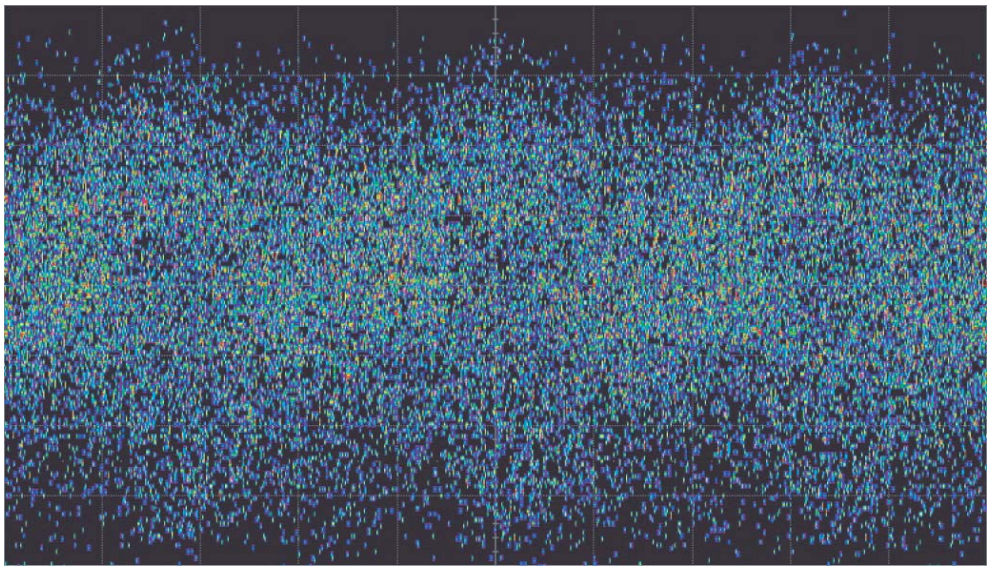


Figure 57: Eve's eye diagram.

of the PRBS sequence. The spacing of the spectral peaks is the inverse of the repetition period of the PRBS sequence. Hence, for a sequence of length 127 bits at a rate of 3 Gbits/s, the peak spacing is of 23.6 MHz [85].

In Figure 58, the spectra of the plain text and the transmission signal are represented. The masking level (α factor) is the same as in Figure 56. We can see that the majority of the frequencies present in the message are masked by the chaotic carrier. Even if the lower frequency components are not completely masked, the chaotic carrier generates enough noise over the rest of the spectrum to render difficult a message extraction.

To qualitatively appreciate the communication quality of the chaotic link, one can spectrally compare the message encrypted by Alice with the message recovered by Bob. Figure 59 presents the two spectrum plots on the same scale. Right off, we note that the general shapes of the two spectra are very close. Bob's spectrum has a peak at the message clock frequency (3 GHz). This peak is about 10 dB stronger than for Alice. The difference in spectral power between the first peak (3 GHz) and the second one (6 GHz) in Bob's recovered signal is caused by a low pass filtering at 2.7 GHz, adapted to a 3 Gbit/s binary data rate. This filtering operation improves the decoding quality by reducing the HF noise

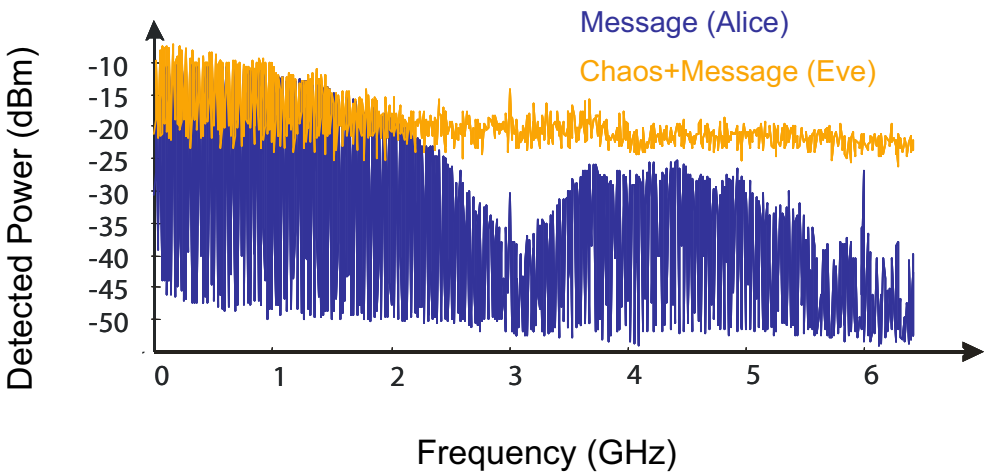


Figure 58: Observed spectra of Alice and Eve for a PRBS7 message at 3 Gbit/s.

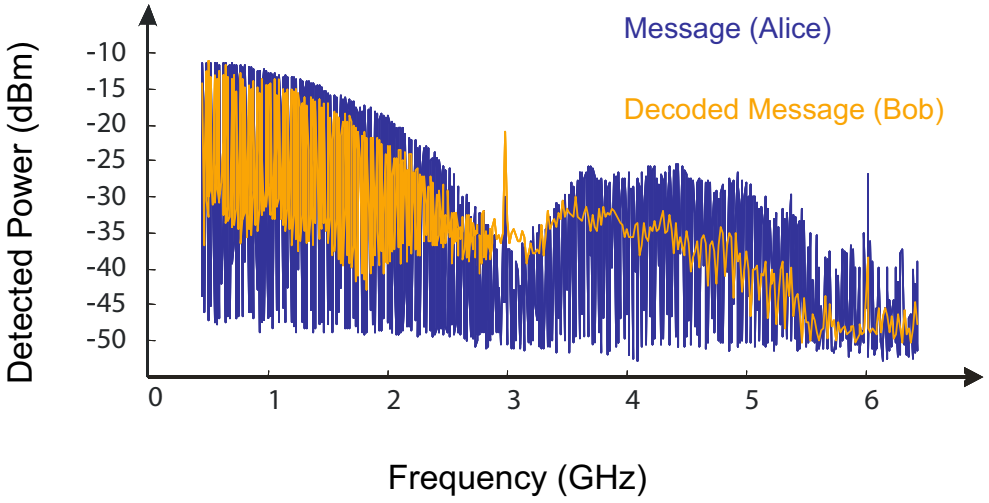


Figure 59: Observed spectra of Alice and Bob for a PRBS7 message at 3 Gbit/s.

present in the system. One of the reasons for this problem is the wideband nature of the system. The wider the spectral bandwidth of the chaos, the greater the noise power resulting from the mismatch between emitter and receiver filter will be. Since noise beyond the message useful frequency is detrimental to the communication quality, the high frequency noise is filtered out.

4.3 Telecom network encryption integration

The encryption we propose differs from the classical technics implemented in telecom networks. Instead of taking place on the application layer of the OSI model (layer 7), the encryption now takes place on the physical level (layer 1). In many legacy networks, the header information had to be decoded at each node. Therefore, the encryption that we propose had to be implemented on each link of the secure connection. The evolution of MPLS towards MPλS (the adaptation of MPLS where the carrier wavelength is the label) facilitates the implementation of our encryption technique in an optical network as the chaotic carrier wavelength could serve as the label in the MPλS scheme.

The MPλS simplification from MPLS occurs at the network switches that direct the traffic at each node. Figure 60 presents the principal diagram of an optical switch. The label forwarding tables are established by the signaling protocols before the communication. Therefore, the switch is ready and signals arriving are processed in the following manner:

- The WDM signal is demultiplexed. Each wavelength is separated.
- The label forwarding table is consulted.
- A wavelength conversion takes place if necessary, depending on the wavelength/label of the output signal.
- The signal is directed on the appropriate output fiber with the correct wavelength.

The optical to electronic conversions are no longer required at each intermediate node. With the deployment of all-optical switches supporting MPλS, networks speeds have risen. A signal travels the network without any access to the payload. Therefore, regarding a potential implementation of chaos cryptography in such a network, decryption/encryption of the message at each node would no longer be necessary. The security of the communication would gain in flexibility and in implementation simplicity.

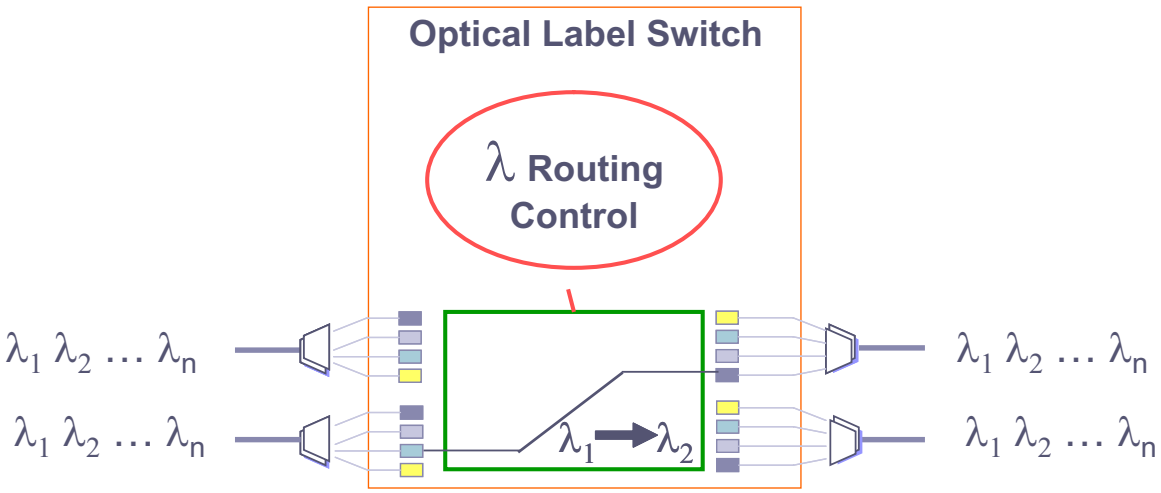


Figure 60: Optical switch for MPλS protocol.

Since the carrier wavelength does not intervene in the cryptographic system, any wavelength conversion should not influence both the security and the decoding quality of a message.

Note that the use of the light intensity as the only dynamic variable removes any practical problems relative to the experimental control of the optical phase and the light polarization. This constraint is very important in all-optical chaos cryptography systems.

Conclusion

After the presentation and the detailed study of the emitter components in Chapter 3, the third chapter was devoted to the receiver (Section 4.2.1) and the study of receiver synchronization on the emitter oscillations (Section 4.2.2) with the proper parameter tuning (gain β, phase ϕ, delay T). With the matched components already selected during the study of the emitter, we implemented the receiver open loop architecture and achieved synchronization with the chaotic regime emitter. From the proper parameter values, we studied the influence of their mismatch on synchronization quality [16]. With controlled synchronization, we studied the evolution of the communication quality between emitter and receiver by measuring the bit error ratio (BER) as a function of the message masking factor (α) [35]. The BER was plotted for both the authorized receiver (Bob) and for an eavesdropper (Eve).

We now possess a cryptographic system that has the potential to be deployable in modern optical networks. Indeed, the wide bandwidth that our system presents offers a real-time encryption technique for high bit rate applications. Our system implements a physical layer encryption that can be deployed over wavelength switched networks such as MPλS networks. The communication quality is dependant on the ability of the receiver to replicate the emitter oscillations. Good parameter matching ensures good communication quality. The tuning precision required for each parameter sets the communication security. The higher the required precision, the harder good synchronization is to achieve, but also harder for a spy (Eve) to find the cryptographic key formed by the set of parameter values. Therefore, a compromise exists between the ease of implementation and the system security. A high synchronization quality will make possible the reduction of the relative power of the message, hence, afford better masking in the chaotic carrier. An authorized receiver (Bob) can actually decode with a BER of $7 \cdot 10^{-9}$ while Eve cannot extract any message information via a direct detection of the transmission signal.

CHAPTER 5

SYSTEM LIMITATIONS AND IMPROVEMENTS

Chapter 4 presented the performance of the chaos encryption system. We studied the synchronization quality of an emitter operating in a chaotic regime and an appropriate receiver, to establish a communication under the best possible conditions. The communication quality was evaluated by the BER as a function of the message masking rate. We were able to establish a limit separating secure communication from non-secure.

Starting from this reference point, we wish to identify, in this chapter, the principal limitation of this system. The limitations affect the transmission distance (limited mostly by the dispersion), the synchronization quality (limited by residual parameter mismatch), and the vulnerability to cryptanalysis. A first series of cryptanalysis attacks will be described with the objective of building a pirate system.

Improvements are then proposed to overcome the limitations previously outlined. A dispersion compensation is implemented to increase the transmission distance. Filter parameter control is also imposed as well as component noise suppression. The impact of these improvements are studied experimentally. Finally, a system architecture evolution of the receiver is proposed to guard against specific cryptanalysis attacks.

5.1 Limitations on system performance

The quality of the encryption is limited by multiple effects. We explore the system security limitations by considering: (1) the problems stemming from the transmission of a signal from emitter to receiver, (2) the limitation stemming from the synchronization quality, and (3) the confidentiality limitations by examining the system robustness to a cryptanalysis attack.

5.1.1 Transmission

The chaos cryptography system performs synchronization with analog signals. However, various deformations interfere with the signal during propagation through the fiber link. The high sensitivity of chaotic systems is an incitation to study the deformations of the transmitted signal and the induced synchronization loss, or, at the least, the sharp degradation of the synchronization quality and the communication quality.

To analyze quantitatively the behavior of our system in a telecom setting, we proceeded, in collaboration with the University of Athens, to study our system while separating emitter and receiver by a long fiber distance.

Two 50 km fiber modules were characterized in order to permit a study over both 50 km and 100 km. Each module is composed of a 50 km single mode fiber (SMF) spool, an erbium doped fiber amplifier (EDFA), and an optical band pass filter. A spool of dispersion compensated fiber (DCF) can also be added. The characteristics of these single mode fiber spools (SMF1 and SMF2) that compose each module are summarized in Table 3.

Table 3: SMF transmission modules characteristics.

Fiber	SMF1	SMF2
Length (km)	50.7	49.4
Dispersion at 1550 (ps/nm/km)	16.806	16.953
Total dispersion (ps)	851.24	837.89
Optical losses (dB)	9.9	9.8

The EDFAs compensate the signal losses due to the fiber attenuation. Optical filters are placed after each EDFA to limit as much as possible the amplified spontaneous emission noise (ASE). Each transmission module can be represented by the architecture of Figure 61.

The experiment is carried out in two steps. The first one is identical to the one in Section 4.2.3: a pseudo-random bit sequence (PRBS) at a 3Gb/s rate is encrypted by the emitter, then decrypted at the receiver. The BER is directly measured in "back-to-back" configuration, without any transmission distance between emitter and receiver. The second step includes the transmission module (Figure 62). In both cases, the message amplitude

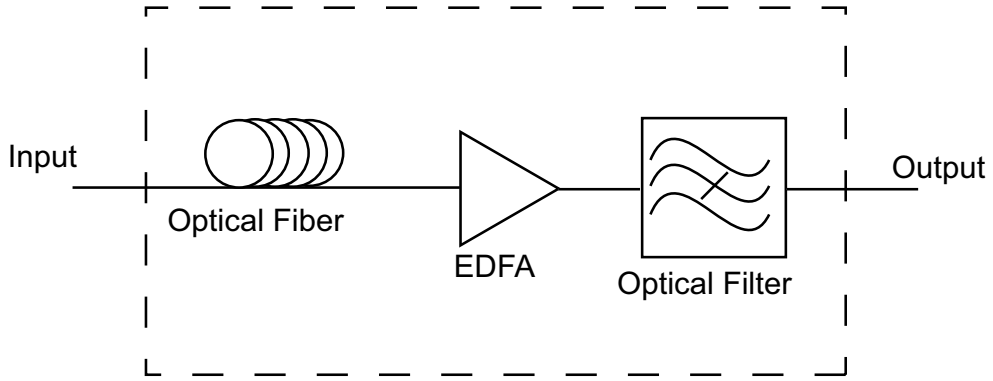


Figure 61: Transmission module.

is adjusted to be properly masked during the transmission. The α parameter is set to 1.3 according to the results of Figure 55.

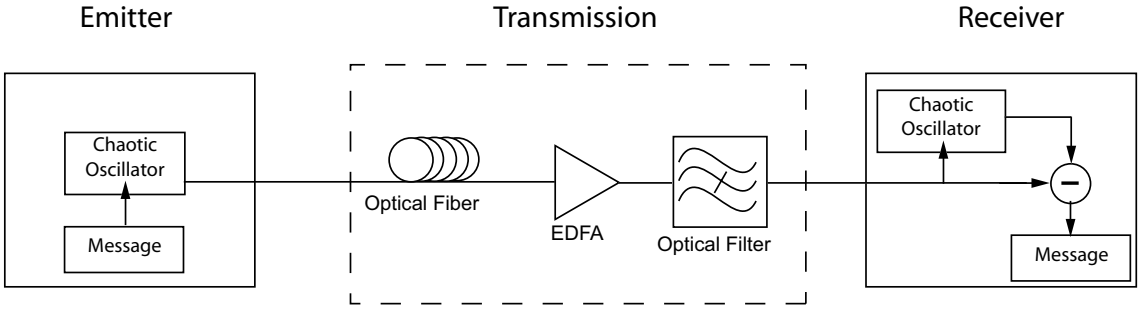


Figure 62: Transmission schematic diagram.

Figure 63 presents the eye diagram of the transmitted signal. The receiver detects this signal after either a 50 or a 100 km transmission.

5.1.1.1 Transmission over 50 kilometers

Before insertion of the transmission module, the BER was measured at 10^{-5} in non-optimal experimental conditions, after a displacement of the experimental setup to Greece. A first transmission experimentation with 50 km of single mode fiber, SMF1, without dispersion compensation, yields a high BER, greater than 10^{-2}. This communication quality level is much below acceptable limits for optical communication. A spool of DCF fiber is then inserted to correct for the dispersion effects. The characteristics of this fiber spool are given in Table 4.

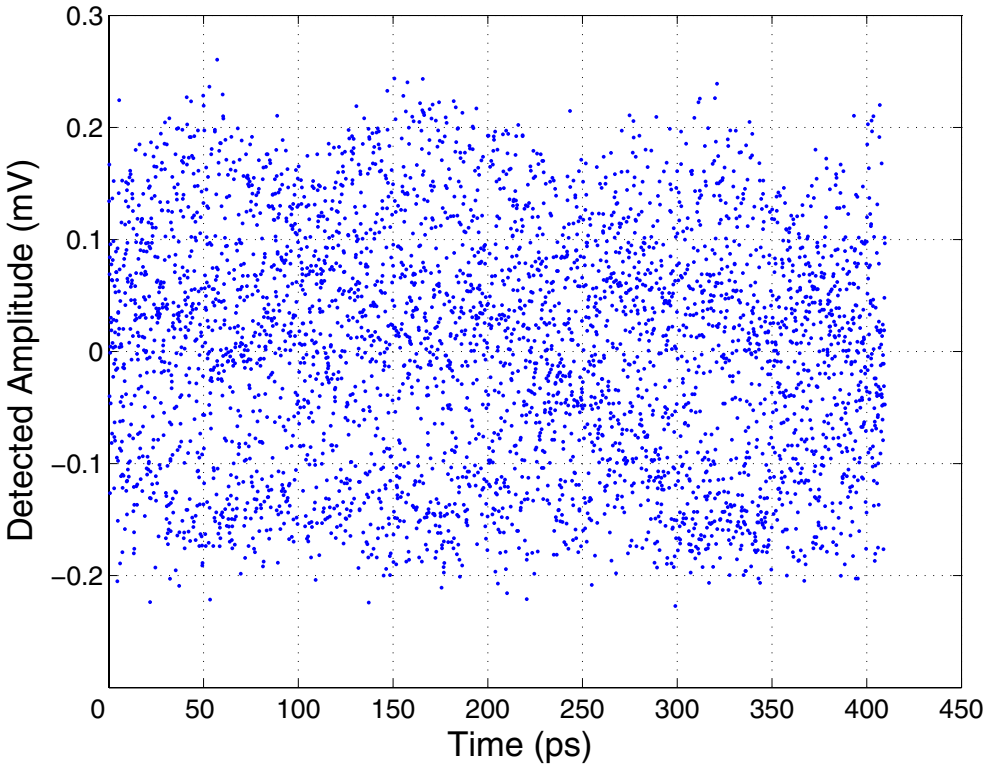


Figure 63: Encrypted signal eye diagram, $\alpha = 1, 3$.

Table 4: DCF transmission module characteristics.

Fibre	DCF1
Fiber length (km)	6.192
Dispersion at 1550 (ps/nm/km)	−137.9
Total dispersion (ps)	853.15
Optical losses (dB)	3.8

The DCF fiber was chosen to compensate the dispersion effects of module SMF1. The total residual dispersion after dispersion compensation is less than 2ps and is considered negligible. After 50 km, the BER is then measured to $2 \cdot 10^{-5}$. The eye diagram obtained at the receiver, after decoding, is presented in Figure 64.

Different frequency signals propagate at different speeds in optical fibers: the fiber index varies as a function of wavelength. This distortion results in a temporal broadening of the signal during propagation. The effects of the dispersion phenomenon become higher as

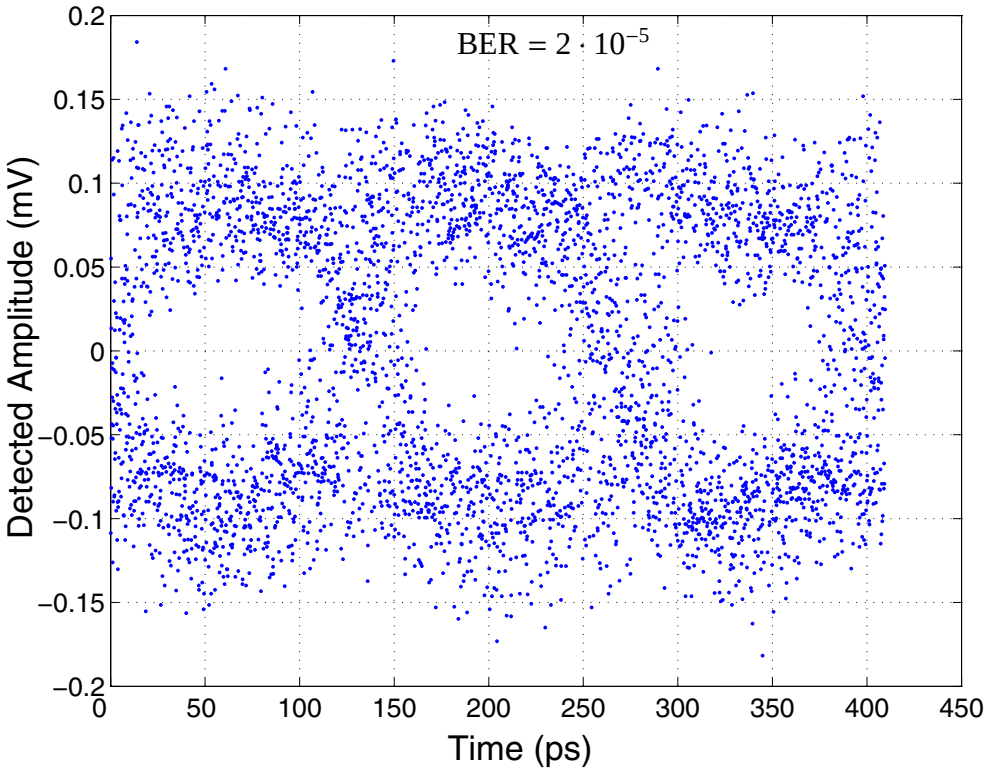


Figure 64: Eye diagram after 50 km transmission and dispersion compensation (BER = $2 \cdot 10^{-5}$).

the bandwidth of the signal increases. For the transmission of chaotic signals, we can observe degradations of the synchronization quality during transmission over long distances. A DCF fiber compensation helps palliate this problem.

5.1.1.2 Transmission over 100 kilometers

The same experiment is performed with 100 km of monomode fiber (SMF1 + SMF2). The BER of the decoded message is unsatisfactory. Once again, DCF fiber is inserted on the transmission line to compensate the dispersion.

After 100 km, the signal degradation is greater. The measured BER is $5 \cdot 10^{-4}$ in the same experimental conditions (Figure 65). Empirically, a 100 km transmission, even with dispersion compensation, increases the BER by an order of magnitude.

The same experiment was reproduced starting from a back-to-back configuration BER

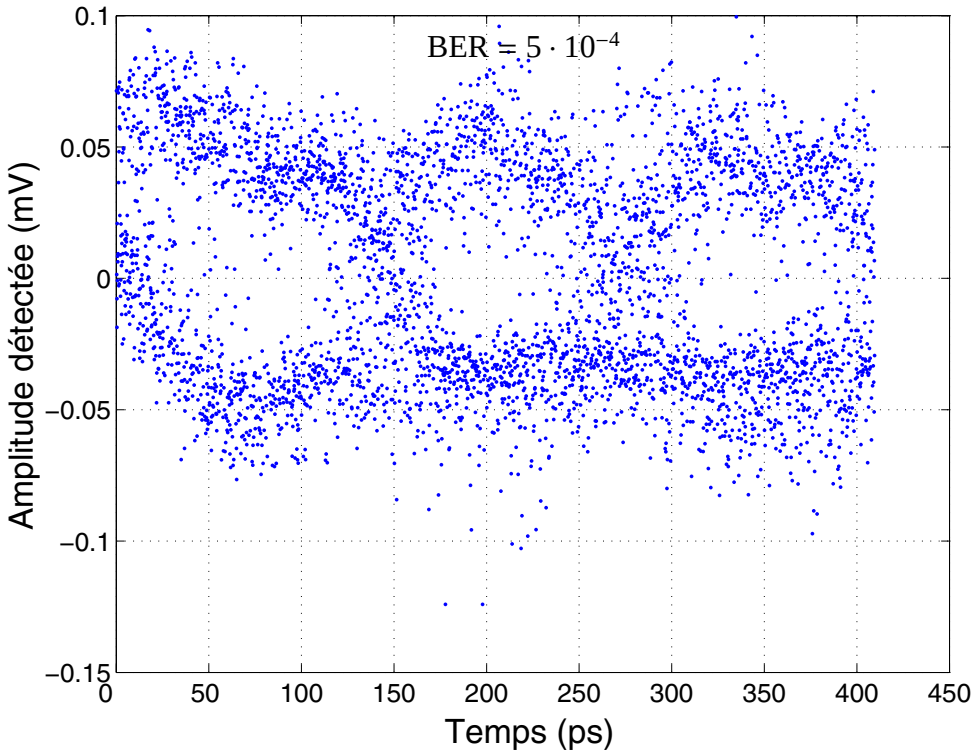


Figure 65: Eye diagram after 100 km transmission and dispersion compensation (BER = $5 \cdot 10^{-4}$).

of $6 \cdot 10^{-7}$. A 100 km transmission with a BER of $8 \cdot 10^{-6}$ is obtained from these synchronization conditions (Figure 66). A BER increase of a power of 10 is observed again.

Through these various experiments, we see that signal transmission translates naturally as BER increases. On the relatively short distances that the system was tested on, the BER decrease is relatively small (an order of magnitude, typically). Yet, for longer transmission distances, the BER penalty might become prohibitive. More systematic tests should be conducted, as well as theoretical and numerical modeling studies concerning the evolution of a chaotic optical signal with very broad RF spectrum (tens of GHz). The phenomena to be considered in this study are the dispersion, the various noise types as well as the distortions due to EDFA. A possible solution to this transmission problem could be solved with a lower BER in the back-to-back configuration, which translates to a better back-to-back synchronization quality. We will study this later in this chapter, in Section 5.2.

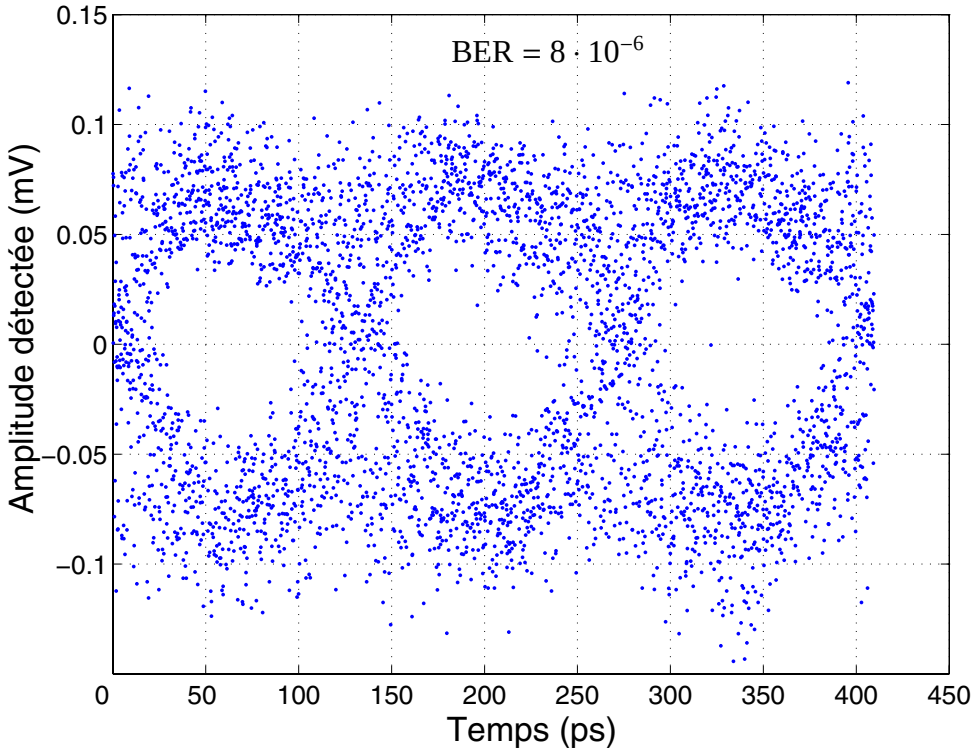


Figure 66: Eye diagram after 100 km transmission and dispersion compensation (BER = $8 \cdot 10^{-6}$).

5.1.2 Synchronization

We already presented in Chapter 4 the study of the influence of certain system parameters (gain, delay, phase) on the synchronization quality and the difficulty of proper tuning. We will now examine the problems stemming from bandwidth mismatch as well as the problems linked to component mismatch. We will see how a common solution can be implemented to increase system performance.

5.1.2.1 Parameter matching

We remember from Section 4.2.2 that the system synchronization quality is −18dB at best. Other opto-electronic systems with different chaotic dynamical variables present better results. For example, wavelength chaos reaches a synchronization level of −20dB [57]. The best result so far is coherence modulation chaos with −36dB [59]. Yet, this setup is limited in bandwidth when compared with the intensity chaos. This narrower bandwidth also

cuts down on the noise present in the system and is one of the factors leading to the better synchronization quality.

Our chaos replication ability is limited. We saw the influence of the optical power P, the phase difference ϕ resulting from the bias voltage, and the delay T on the synchronization. Two parameters remain whose influence has not been studied. The first one is the non-linear function f_{NL}. Because of the modulator type we used, f_{NL} is of a $\cos^2$ form. Unfortunately, we have no means of exerting any control on the matching of the non-linear functions of the emitter and the receiver. The second parameter is the system bandwidth represented in Equations (29) and (34) by θ and τ. Again, we have no experimental control on the individual filter functions of each component of the receiver to match them to those of the emitter. The only control we have is to force the system filter function by restriction to the bandwidth of a calibrated filter, with the same filter at both emitter and receiver. The experimental study is presented in Section 5.2.

5.1.2.2 Component noise

We just saw in Section 5.1.2 the limitations associated with the synchronization quality. Part of the error comes from the combination of the various parameter mismatches, which leads to errors in the chaos replication process. Errors are also induced by the noise produced by the components, noise which is necessarily different and uncorrelated at the emitter and the receiver. The principal active elements of the system are the photoreceivers and the RF amplifiers. They generated the majority of the noise present in both emitter and receiver. We detail first the origins of the noise in the photoreceivers before moving on to the RF amplifiers.

The photoreceivers we use are composed of a PIN photodiode and a linear transimpedance amplifier. The PIN photodiode transforms the optical signal into an electrical current with a high sensitivity. For an incident optical power P_in, this electrical current, flowing through an impedance, can be expressed as: $I(t) = I_p + i_s(t)$, where $I_p = RP_{in}$ is the average current and $i_s(t)$ represents the variations of the photodiode current due to the shot

noise. The variance of the shot noise is given by the equation: $\sigma_s^2 = 2qI_p\,\Delta f$, with Δf as the effective noise bandwidth depending on the photoreceiver structure, and q is the elementary charge. This corresponds to the intrinsic photoreceiver bandwidth if current fluctuations are measured. Since the dark current also generates shot noise, this contribution is taken into account by replacing I_p by $I_p + I_d$ with the following equation as a result:

$$\sigma_s^2 = 2q\,(I_p + I_d)\,\Delta f. \tag{60}$$

The value σ_s is the mean quadratic value of the photocurrent resulting from the shot noise [3].

Experimentally, we cannot control the noise emission in the system. The only available approach is to limit the noise to the frequencies of the message by filtering, thus, rejecting all out of band noise. The insertion of a low-pass filter in the chaotic feedback loop has a double effect: all the spectral components that are out of band (including the out of band noise) are highly attenuated, and the filters impose their spectral response to the system. This filtering enables an extra limitation on top of the component response. We can observe very clearly the effects of the filtering when comparing the electrical bandwidth of the two systems with and without the low pass filter present ($f_c = 2.7$ GHz) in the chaotic feedback loop. Without filtering, the bandwidth is of 6.5 GHz whereas, after filter insertion, the bandwidth is reduced to 3 GHz. By imposing this response, the filter gives us independent control on an extra system parameter. We will detail the filter frequency response and the chaotic dynamic spectrum obtained in Section 5.2.1.

Since we have considered the system limitations in terms of communication quality, we now examine the confidentiality limitations.

5.1.3 Cryptanalysis attacks

Communication security is of capital importance in settings ranging from diplomacy to private communications between individuals or business partners.

Cryptography and cryptanalysis are two sides of the same coin. To evaluate this security, several attacks have been evaluated. First, we study their effects on the original wavelength chaos cryptography system [58] before expanding these results to the system we have studied in the previous chapters.

The bandwidth of the original system spans frequencies starting from DC to several tens of kHz. The system's dynamic is of high dimension (~ 500) because of the sweep of multiple extrema of the non-linear function [37]. The system is modeled by Equation (19) that we rewrite including the message term $m(t)$:

$$x(t) + \tau \frac{d\,x(t)}{dt} = \beta\, F_{NL}[x(t-T)] + m(t). \tag{61}$$

Therefore, the parameters that form the cryptographic key of the system are τ, θ, β, F_{NL} and T. The non-linear function comprises two parameters: the phase ϕ and the shape of the non-linearity. The objective of the cryptanalyst is to identify these parameters in order to duplicate the system to decode the message in real-time by direct detection of the signal on the transmission line.

The approach described in reference [91] successfully identifies three of the five parameters, thus considerably reducing the encryption strength. The cryptanalyst will proceed by steps to identify the parameters one by one, starting with τ.

The parameter τ represents the time constant associated with the high cut-off frequency. This time constant is relatively easy to identify using a simple spectral analysis of the transmitted signal. Indeed, one must only compute the time constant associated with the -3 dB cut-off frequency. Furthermore, some parameter mismatch is acceptable without highly influencing the chaos replication process. Within the cryptanalysis of the wavelength chaos system, the spectral analysis of the transmitted signal yields a value $\tau_{guess} = 9$ ms for a correct value of $\tau = 8.6$ ms, a difference of 5%. The first parameter of the system modeling is therefore identified.

The second parameter to be identified is T, the overall time delay of the chaotic feedback loop. We recall that this delay is composed of the intrinsic delay of each electronic or

opto-electronic component and the specific component performing a pure delay function, a coupled charge device (CCD), for the low frequency systems. The complete feedback loop has a delay of $T = 510\ \mu$s [91].

There are multiple methods to recover the time delay. The first one consists of analyzing the auto-correlation function of the transmission time series. The second one, described by Fraser and Swinney [29], consists of calculating the average mutual information of the transmitted signal for different delay values. A peak appears at the correct delay value. One can then proceed by reconstructing the derivative of $x(t)$. The application of these two methods gives good results with an estimated delay value of $T_{guess} = 514\mu s$. The error is smaller than 1% with respect to the correct value of T. With this precision, the cryptanalyst can proceed to the next step before refining his measure.

With the first approximation of the delay T given by the methods used above, the process can be started for determining the non-linear function used in the chaos generation process. A first approach consists of plotting the primary feedback application of the transmitted signal. The measured wavelength is plotted as a function of itself at a time T_{guess} later. The general form of the non-linearity then appears. Yet, the plot gives a blurred representation and does not allow for a precise determination. Another procedure can be adapted to achieve better results. This method can be decomposed into two steps. With the following double assumption: $m(t) \ll x(t)$ and $|dm(t)/dt| \ll dx(t)/dy$, Equation (61) can be written as:

$$x(t) + \tau \frac{dx(t)}{dt} \approx \beta F_{NL}[x(t-T)]. \tag{62}$$

In a physical sense, these assumptions mean that the message does not influence locally the system dynamic. The analysis of this time series makes possible the computation of the function $X(t) = x(t) + \tau dx(t)/dt$. This function $X(t)$ is approximately $\beta F_{NL}[x(t-T)]$ from Equation (62). Therefore βF_{NL} can be reconstructed using a series development. This method gives good results, yet not precise enough to use them with Equation(61). The error between the reconstructed F_{NL} function and the original can reach the 25% mark. However,

the procedure outlined above gives us necessary information to proceed to the second step of obtaining F_{NL}.

With the information gained during the first step, the cryptanalyst can make the assumption that the non-linear function βF_{NL} is of the $\sin^2$ form: $\beta F_{NL}(\lambda) = A\sin^2(B\lambda + C)$, where A, B and C are parameters to be determined. The second step consists of determining these three parameters with the necessary precision to obtain a non-linear function as close to reality as possible. With this objective in mind, we compute the approximation error matrix:

$$E_{i,j,k} = \sum_{l=1}^{N} \left[\beta F_{NL1} - A_i \sin^2(B_j \lambda^l + C_k)\right]^2, \tag{63}$$

where N is the number of points considered in the previous step. The results of the preceding step allow us to center the computation around expected values. The minimum point of the error matrix gives values for A, B and C. The cryptanalyst then has all the parameters with necessary precision to use Equation (61) to decipher the message [91].

The techniques presented here were developed based on the wavelength chaos system described in [58] and are also applicable to other chaos generators, such as the intensity chaos, for example. Therefore, we applied the average mutual information technique [92] to a chaotic trace generated by our system. This technique measures the interdependence between two variables. In the present case, we look at the chaotic trace $x(t)$ and its delayed version $x(t - t_0)$. If they are not completely independent, the average mutual information function will present a peak at $t_0 = T$, where T is the exact value of the delay. Since $x(t)$ and $x(t - t_0)$ are linked by Equation (29), the average mutual information function plotted as a function of t_0 will present a peak at $t_0 = T$. An eavesdropper using this technique computes a delay value of T_{guess} equal to 42.22 ns. Figure 67 shows a very clear peak at this value of the time delay. As we have seen in Figure 38, the emitter delay was measured experimentally at 42.15 ns. The difference between true and estimated values is of 0.07 ns. Referring ourselves to Figure 52(b), we observe that a delay mismatch of this size introduces very large decoding errors. Even if the eavesdropper has a good estimate of

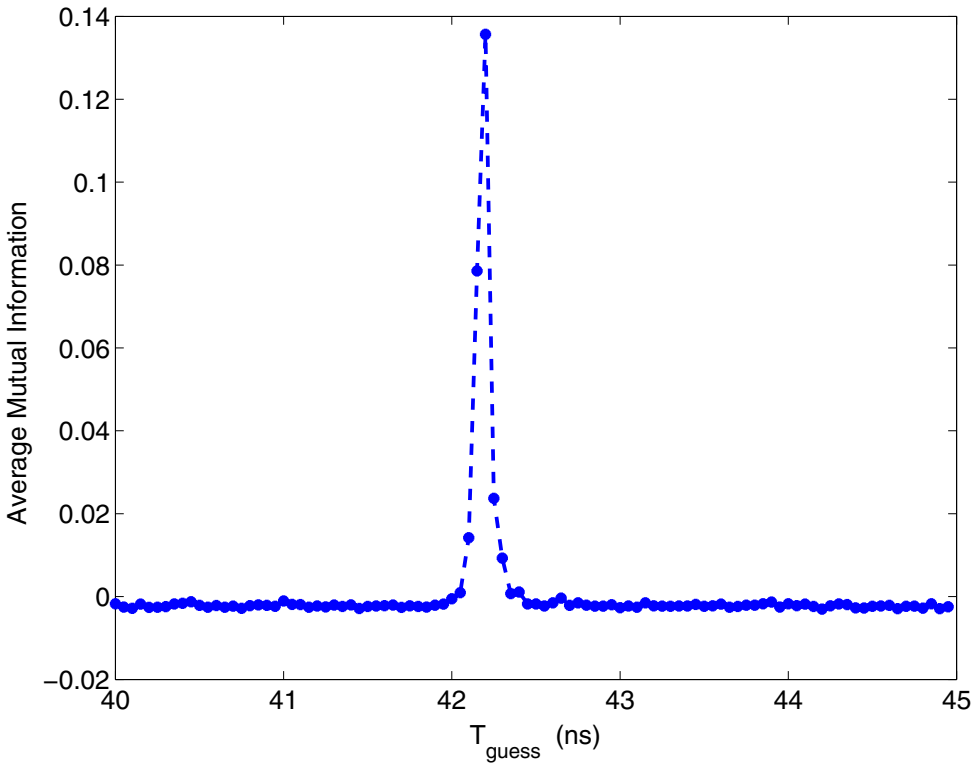


Figure 67: Average mutual information extracted from an experimentally transmitted signal.

the delay value, the precision of the computation is not sufficient to proceed directly to the next stages of the method described previously. He will need to get a better approximation (possibly by trial and error) before proceeding.

Without saying that the security of system is broken, we have to acknowledge that security is compromised since the cryptanalyst is in possession of the correct value for at least one parameter (τ) and a good estimata of the delay. These values give him a starting point to identify the value of T, before proceeding to identification of the non-linearity.

5.2 Possible improvements

In the previous chapter (Section 4.2.2), we studied the synchronization quality evolution as a function of the mismatch of three parameters present in the equations describing the emitter (29) and the receiver (34). Therefore, three parameters remain on which no control has been exerted: the cut-off frequencies, τ and θ of the system filter function as well as the

shape of the system non-linearity F_{NL}.

5.2.1 Filter

The system bandwidth results from the successive filtering operations of each component of the chaos feedback loop. In the wideband systems with which we are operating, the low frequencies are filtered out. The opto-electronic chain transfer function is therefore of the band-pass type. The time constants associated with the high and low filter cut-off frequencies are denoted τ and θ. The article by Kouomou *et al.* [16] demonstrated that the agreement between emitter and receiver low pass filter characteristics has only a small influence on the synchronization quality. On the other hand, the system synchronization is much more affected by high-pass filter mismatch.

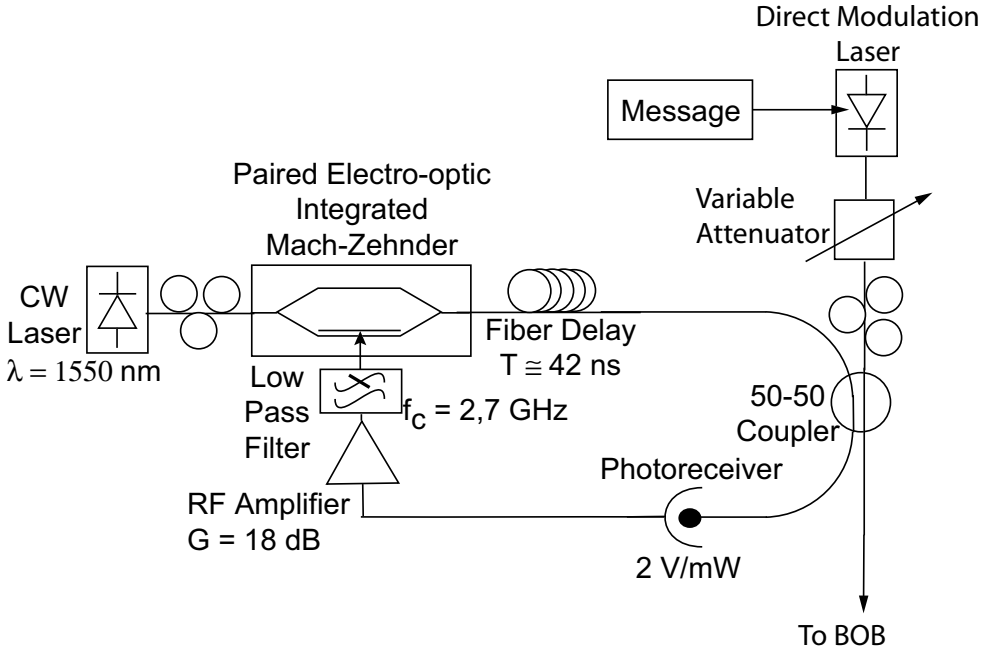


Figure 68: Experimental emitter diagram with filter.

To increase the quality of the telecom link developed in Section 4.2.3, low-pass filters were inserted into the chaos generation loop at the emitter and in the chaos replication elements of the receiver. The diagrams of Figures 36 and 46 become, respectively, Figures 68 and 69.

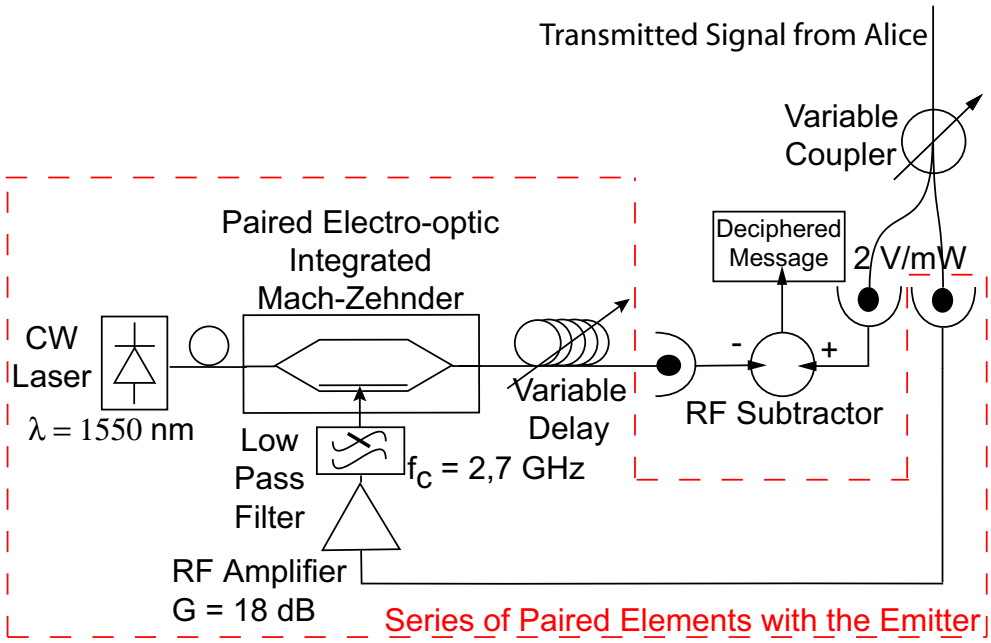


Figure 69: Experimental receiver diagram with filter.

Particular care was given to the matching between the two filter responses. The agreement is so good that the two plots are superimposed in Figure 70.

The two filters are from Picosecond Pulse Labs and are approximate Gaussian filters. Their time response to a step input has very little overshoot ($\approx$ 0.5%) and low residual oscillations, unlike filters with strong band-stop behavior. This characteristic is particularly appreciated: indeed, the filters will not add any oscillations to a system that is already oscillatory by nature [6].

5.2.2 Non-linearity

In our system, the non-linear function performed by the electro-optic modulator plays a central role (Section 3.2.1). The obtained transfer function has a $\cos^2$ aspect. In order for their characteristics to be as close as possible, the two modulators that we ordered were made from the same substrate. The differences, albeit small, are evidenced on Figure 34. Amplitude differences are easily compensated by a gain adjustment to have the same "non-linearity weight" at the emitter and the receiver. The modulator operating point can also be fine tuned by adjusting their bias voltages, V_b. However, any difference of symmetry

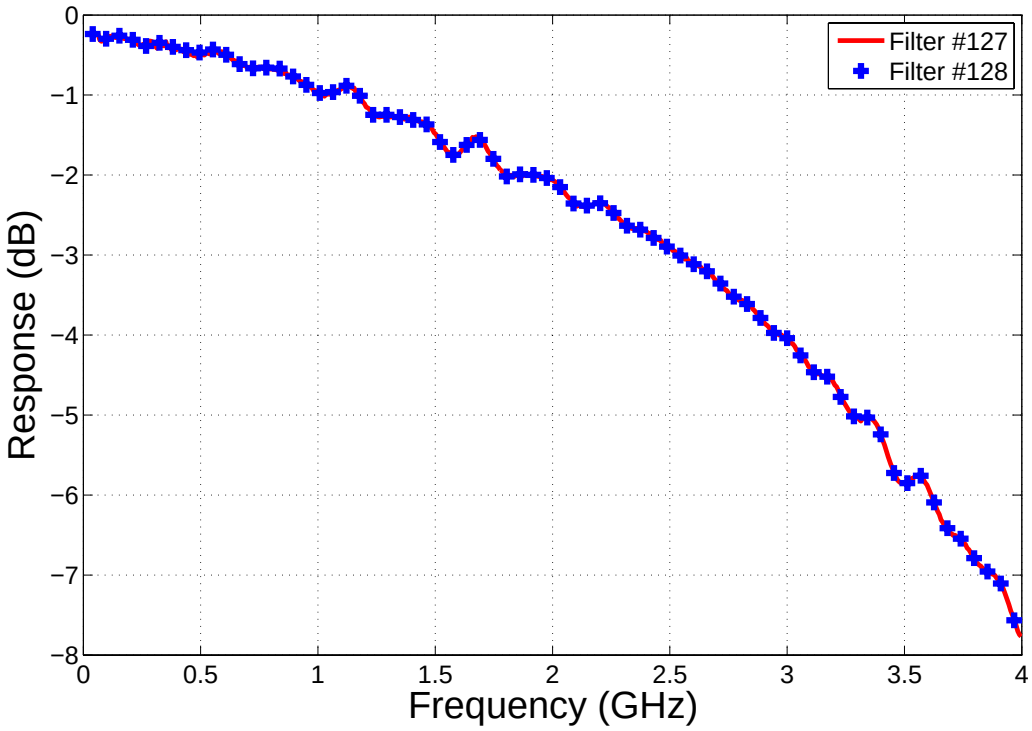


Figure 70: Frequency response of two low-pass filters.

between the non-linear functions cannot be compensated experimentally.

The system also perceives the non-linearity of the electro-optic modulators differently depending on the light polarization at the input. The modulators have two main polarization axis for which the modulation efficiency is maximum. In our case, since modulation is synonymous with non-linearity, polarization must be adjusted properly. The light polarization at the modulator input is regularly controlled to compensate and correct for random fluctuations resulting from, on short or long time scales, mechanical constraints on the fiber and thermal variations of the environment.

5.2.3 Noise suppression

The filters described above (Section 5.2.1) play a double role. They permit the matching of emitter and receiver bandwidth by imposing their own bandwidth. The downside is that the chaos spectrum is reduced and the cypher message spectrum as well. Indeed, one

condition for the masking to be efficient is its complete spectral overlap with the message. The introduction of a low-pass filter in the chaotic feedback loop also permits the decrease of the broadband noise generated by the components by filtering the noise that is outside of the message spectrum.

The message remains the same as in one of the experiments of Section 4.2.3: a PRBS message of 127 NRZ coded bits at the frequency of 3 GHz. Since the frequency band covered by the chaotic dynamic stretches to 6.5 GHz, roughly half of the system bandwidth is not strictly necessary for message encryption. The noise generated by the electronic components is also present at frequencies beyond those of the message.

5.2.4 Experimental improvement

The system represented by the Figures 68 and 69 is studied experimentally and compared to the initial system of Chapter 4 (Figure 54) to highlight the advantages and the drawbacks of each system.

To assure ourselves of similar dynamical behavior between the two systems (i.e. with and without low pass filter in the chaotic feedback loop), bifurcation diagrams are used to compare the two systems. The spectrum of the generated chaos from the system with the low pass filter is presented, before concluding with BER measurements.

5.2.4.1 Effects of filtering on the chaotic dynamic, route to chaos

To compare the dynamics of the systems with and without filtering, their bifurcation diagrams are plotted under various conditions with the emitter laser diode power (P_1) being progressively increased to a maximum. The histogram of the time trace is recorded. This recording technique differs from the one of Section 3.2.2. We now record the chaotic signal directly in the optical domain (measured optical power) with an optical detector DC - 30 GHz on a repeating oscilloscope with which we construct, after multiple triggering, the histogram for each value of β, directly proportional to the optical power P_1. In Section 3.2.2, we were recording an RF signal after the band-pass filtering of an amplified photodiode and

an RF driver. Therefore, the DC component of the signal was filtered out. The measurement heads of the fast oscilloscope have a bandwidth of 5 GHz and also filter the signal. The presence of the DC component in the signals that were used for the construction of Figures 71, 72, 73 and 74 explains the difference in aspect of the diagrams of Chapters 3 and 5.

Figures 71 and 72 were obtained under the same conditions of power (P_1), modulator bias voltage ($V_{B1} = 2.85V$) and delay ($T = 42.15$ ns). The only difference (for Figure 72) is the presence of filter (# 127, Figure 70) in the chaotic feedback loop. The two bifurcation diagrams, with and without filter, are very close. The only difference is found in the contrast level of each figure. We observe a stable regime from 0 to 17% of P_1. As P_1 further increases, the system undergoes a series of bifurcations and multi-periodic behaviors leading to a chaotic dynamic as P_1 reaches 65% of its maximum value.

The bifurcation diagrams for the systems with and without filter are again constructed, but for a different modulator bias voltage ($V_{B1} = 0.7$ V). The power P_1 of the laser remains the same, as does the system delay. The system is then in a different dynamical configuration which constitutes another route to chaos, different from that of Figures 71 and 72. Figures 73 and 74 present the constructed diagrams. The first bifurcation occurs later, for a more important optical power than previously, at 22% of P_1 instead of 17%. The bifurcation also appears sharper, the rupture in the dynamic more abrupt. Subsequent dynamical evolution occurs by successive bifurcations. Starting at 62% of P_1, we observe a bifurcation diagram structure that is similar to that of Figure 71 and 72.

For these two different modulator bias voltages, the presence of a low-pass RF filter within the chaotic feedback loop does not modify the chaotic dynamic or the evolution of the system towards a chaotic behavior.

5.2.4.2 Effects of filtering on the chaotic dynamic, spectral width

For each of the two chaotic dynamics obtained with different modulator bias voltages, we have observed similar behaviors, with and without the presence of a low-pass filter within

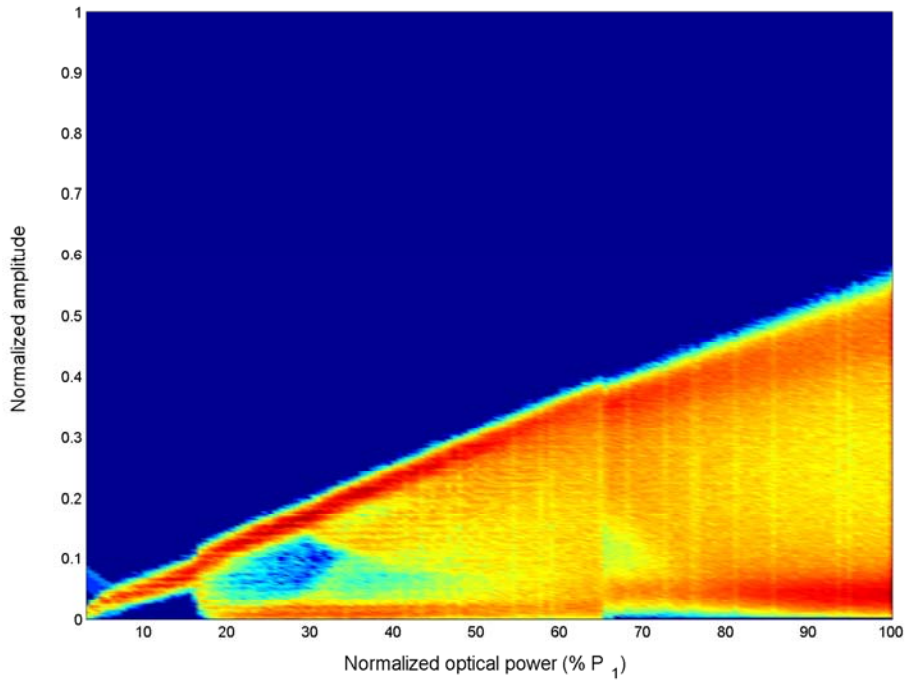


Figure 71: Bifurcation diagram without filter and modulator bias voltage $V_{B1} = 2.85$ V.

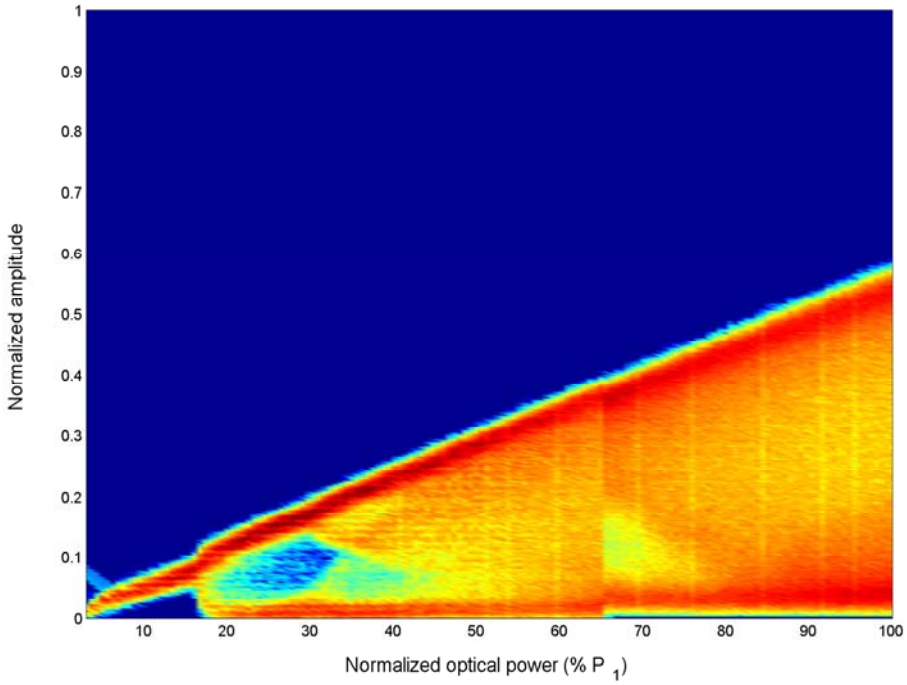


Figure 72: Bifurcation diagram with low-pass filter ($f_c = 2.7$GHz) and modulator bias voltage $V_{B1} = 2.85$ V.

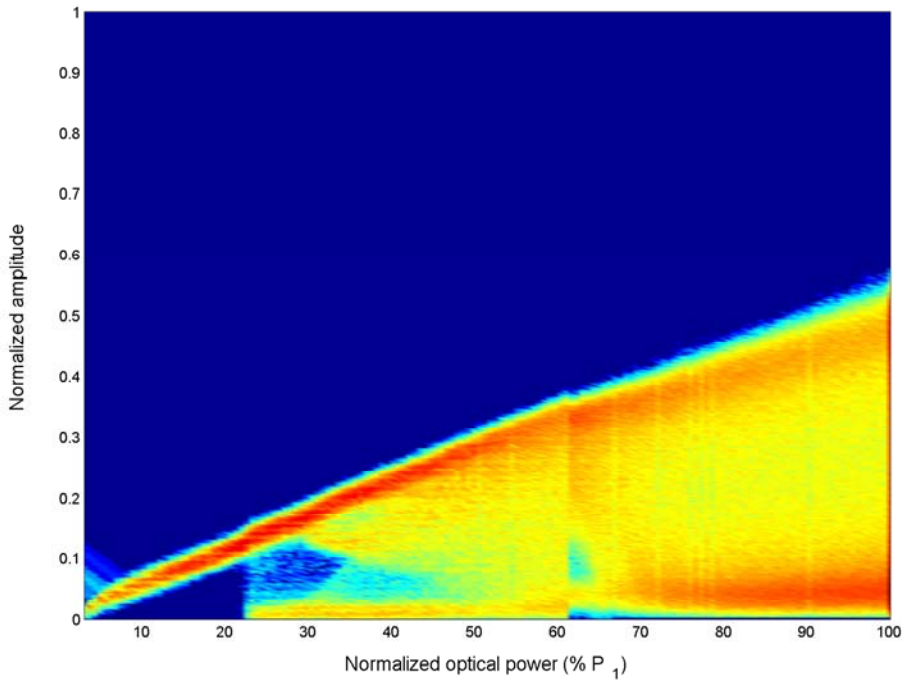


Figure 73: Bifurcation diagram without filter and modulator bias voltage V_{B1} = 0.7 V.

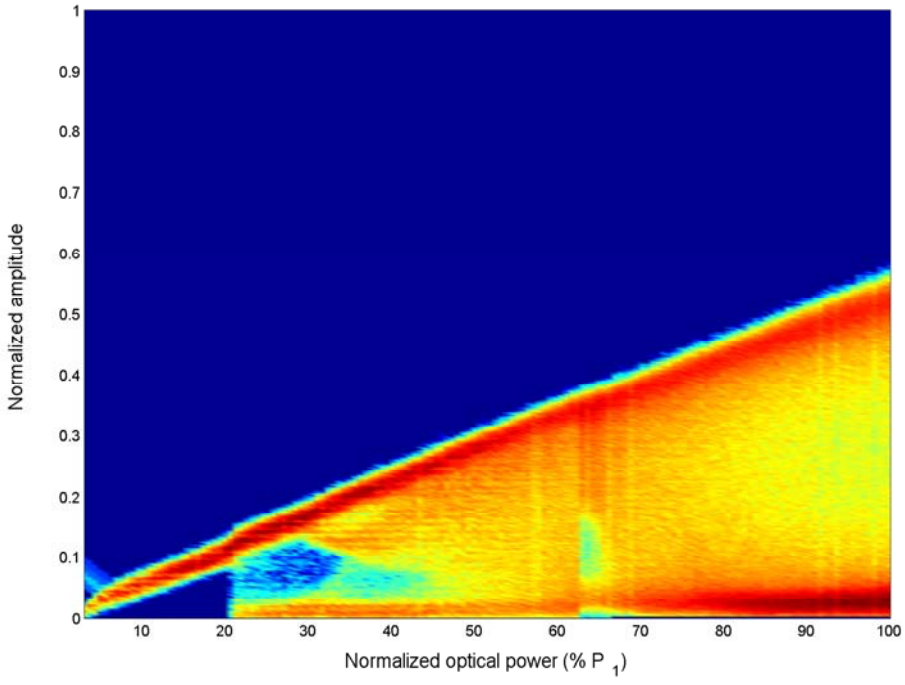


Figure 74: Bifurcation diagram with low-pass filter (f_c = 2.7GHz) and modulator bias voltage V_{B1} = 0.7 V.

the chaotic feedback loop. The only noticeable difference, one the bifurcation diagram does not evidence, is the frequency range covered by the chaos. Indeed, when the emitter laser is operated at maximum power, the chaos spectrum for the "unfiltered" system has a -3 dB cutoff frequency of 6.5 GHz (Figure 42). The effects of the filtering are visible on the spectrum displayed in Figure 75 since the -3 dB cutoff frequency is now close to 3 GHz.

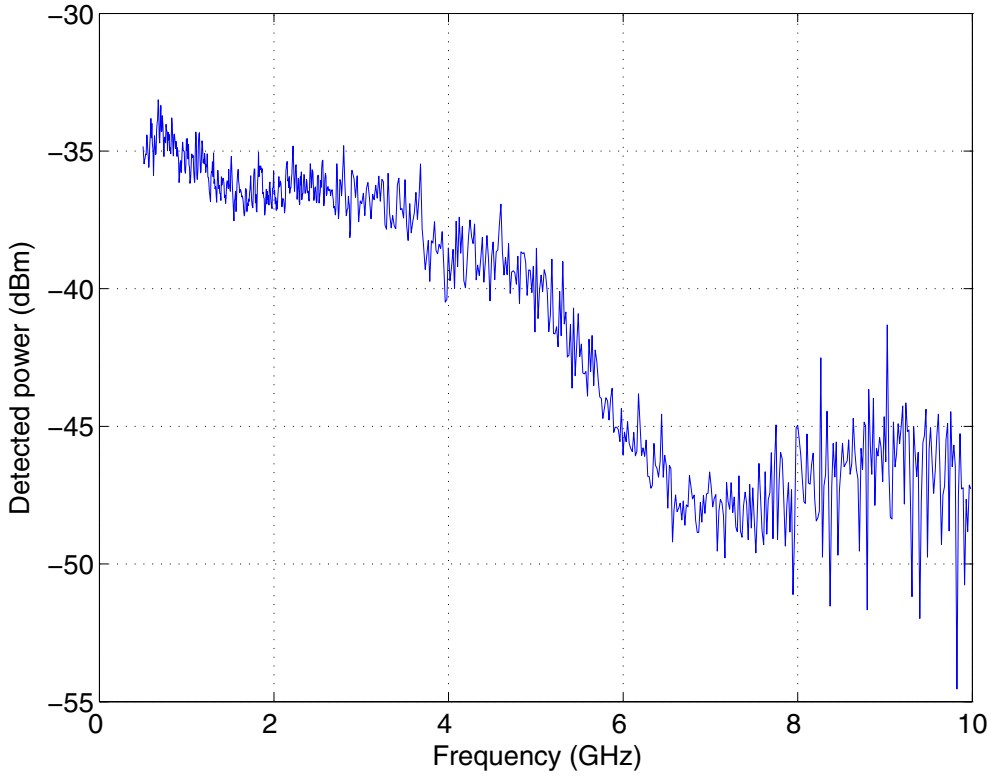


Figure 75: Experimental spectrum of the chaotic dynamics generated by the emitter with a low-pass filter (filter #127) in the feedback loop. P_1 = 6 mW, V_{B1} = 2.85 V, T =42.15 ns.

5.2.4.3 Effects of the filtering on the BER

We have established the similarities between the dynamic behavior of the system with and without a low-pass filter in the chaotic feedback loop. We will concern ourselves with the effects of the low-pass filtering described earlier on the communication quality between emitter and receiver, as measured by the BER. We repeat the experiment described in Section 4.2.3, but with the low-pass filters inserted in the emitter and the receiver, as described by Figures 68 and 69. We quickly recall that the message is composed of a series

of NRZ coded PRBS sequences of length 127 bits, at the frequency of 3 GHz. The BER is measured as a function of the masking coefficient α, quantifying the masking of the message in the chaos.

Two plots of the BER as a function of the masking coefficient are presented in Figure 76. The first plot (solid line) was obtained without any filtering in the feedback loop. This "reference" plot was obtained in exactly the same conditions as the one in Figure 55. For a small α coefficient, the error rate is high. With $\alpha = 0.57$, the BER is measured at $3 \cdot 10^{-3}$. The increase of the masking coefficient decreases the BER to reach 10^{-9} when $\alpha = 1.5$. Comparison of the numerical values to those of Figure 55 is problematic because some components had to be replaced[1]. Yet, the overall aspect of the plot is conserved.

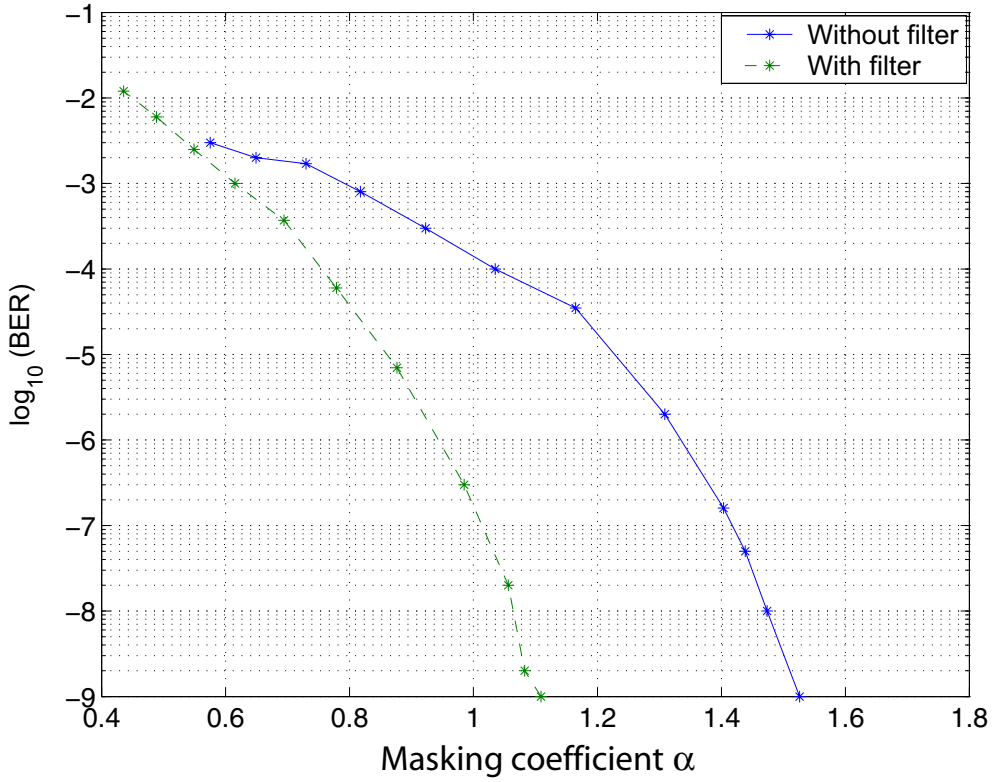


Figure 76: Evolution of the BER with and without RF filter at 2.7 GHz.

When the low-pass filter is inserted in the feedback loop, the BER plot is modified. The initial point, for low α, is roughly the same. For $\alpha = 0.55$, the BER is measured at

[1] A sensitive photoreceiver was damaged by the voltage variations of an unstable generator.

$2.5 \cdot 10^{-3}$. The overall aspect of the plot is also the same. The decrease of the BER as a function of the masking coefficient is much more pronounced when the filter is part of the system. For example, when the masking coefficient is close to 1, the BER is of $3 \cdot 10^{-7}$ whereas, in the absence of filter, the BER is measured at 10^{-4}. A standard BER of 10^{-9} is achieved for $\alpha = 1.1$ with the "filtered" system, contrasting with the $\alpha = 1.5$ necessary without any filtering.

The presence of a filter in the chaotic feedback loop not only increases the communication quality with a notable BER improvement but also contributes to the system security. All of the measurement points are considered secure since all of the measurement points are below the secure threshold determined in the previous chapter (Section 4.2.3) where an eavesdropper can decipher the message by direct detection of the transmitted signal.

In this section, we experimentally evidenced the improvement of the communication quality that the insertion of a low-pass filter in the chaotic feedback loop permits. The problem of the deferred attacks, by progressive reconstruction of the system parameters, is not solved. As we have seen in Section 5.1.3, the eavesdropper can hope to crack the system by analyzing a transmission that he has recorded. He can recreated the chaotic emitter by finding the system parameters that determine the system behavior and that constitute the cypher key. With these parameter values in hand, a spy can then reconstruct a working pirate receiver and decrypt the message.

5.2.5 Confidentiality increase possibilities

As seen in Section 5.1.3, some methods of time series analysis [44, 91] made for the determination of certain experimental parameters of the chaotic emitter, and therefore, potentially, the unauthorized recovery of the transmitted signal. Transmission confidentiality is no longer assured.

One solution to remedy this limitation was proposed by Min Won Lee *et al.* [61]. Modifications were made to the architecture of the system presented in [60] to increase system security.

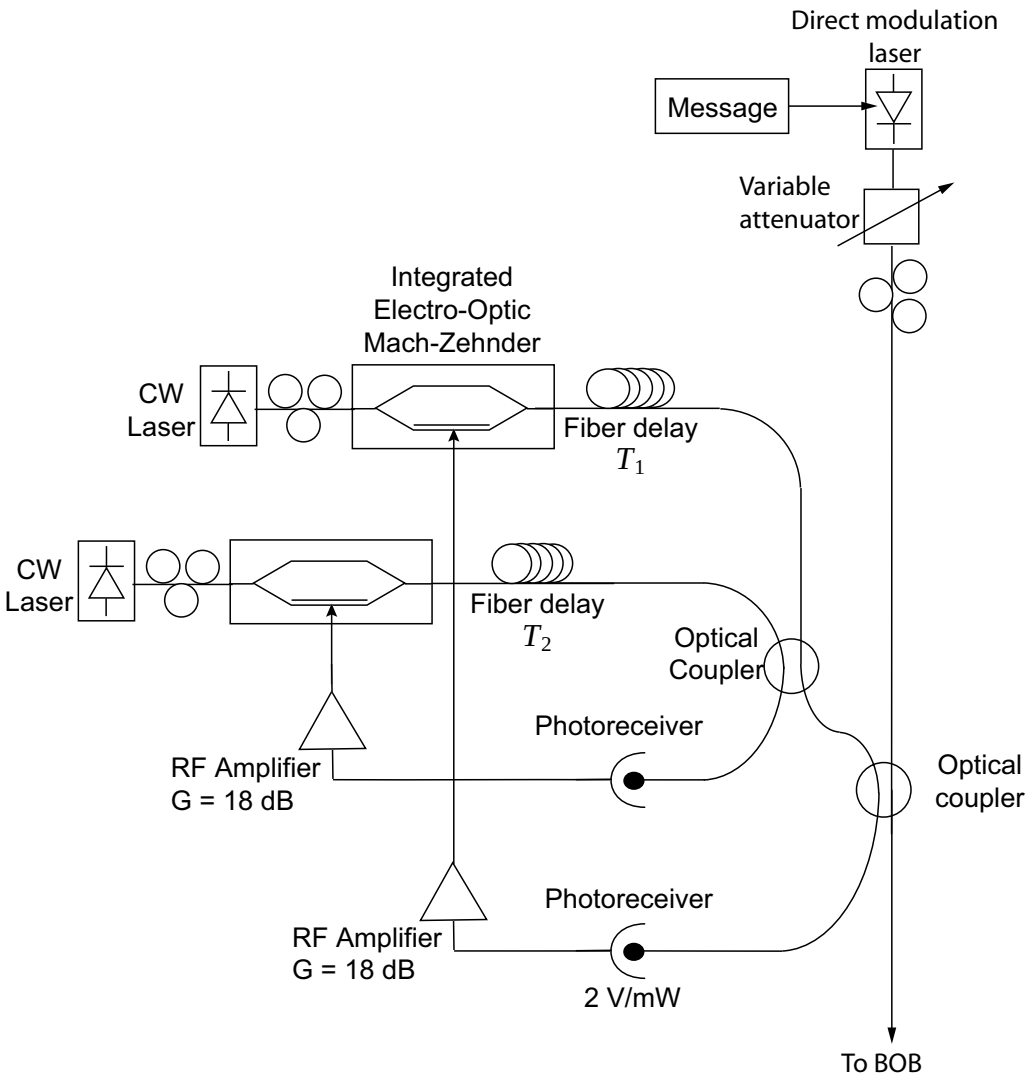


Figure 77: Intensity chaos system diagram with two delays and two non linearities in the feedback loop.

The objective of these modifications is to complicate the task of the cryptanalyst that is trying to obtain information on the system delay and on the non-linearity. Thus, the feedback loop that originally had one non-linearity associated with a single delay is doubled. The chaos complexity is more important than with single delay systems. The confidentiality increase is synonymous with a higher number of positive Lyapunov exponents [61]. This double architecture of the feedback loop denies results from the methods described in [91]. The double-branch feedback loop originally proposed for the coherence modulation chaos, results in the diagram of Figure 77 for the intensity chaos case. Such a system,

analogous to the one developed for the coherence modulation chaos, but for the intensity chaos, has not yet been studied. Current cryptanalysis methods [92] do not yield good results when applied to the equivalent system developed for wavelength chaos. Verifying whether or not this increase of security is the case for intensity chaos would be interesting.

Conclusion

In this chapter, we presented essentially work done to characterize the system limitation in terms of synchronization and security (Section 5.1). These limitations are in terms of synchronization quality (12 dB maximum), transmission distances (100 km) and resistance to cryptanalysis attacks using the average mutual information.

We have systematically proposed improvements to the initial system in order to overcome several principal limitations (Section 5.2). To increase the transmission distances, dispersion compensation was implemented by combining SMF and DCF fibers. We measured an error rate of $8 \cdot 10^{-6}$ after transmission over 100 km of fiber. A solution to increasing the transmission quality consists of inserting matched band-limiting filters ($f_c = 2.7$ GHz) in the chaotic feedback loop at the emitter and within the chaos replication process at the receiver. These filters do not modify the nature of the chaotic dynamics of the system, but impose a reduced bandwidth identical for both emitter and receiver. For a same masking coefficient α, a lower BER can be achieved, which is an indication of a higher communication quality. To guard against a spy determining the value of the system delay T by using the average mutual information technique, we proposed a system architecture with a two-branch feedback loop with two non-linear functions.

CHAPTER 6

BEYOND THE NRZ FORMAT

In the previous chapters of this dissertation, the focus was placed on the emitter and receiver of the chaos communication system. The emitter characteristics were detailed in Chapter 3, where special consideration was given to establishing the emitter's chaotic nature. Chapter 4 examined the receiver as the natural complement to the emitter. The synchronization quality of one to the other was measured as a factor of specific parameters (e.g. gain, delay, phase). The quality of the communication link as attested by the bit error ratio (BER) was measured as a function of message amplitude. Chapter 5 examined the system limitations in terms of transmission and security and proposed solutions to them.

Throughout this work, the message was an NRZ-coded PRBS of length $2^7 - 1 = 127$ bits. This message format is very conventional and the simplest to generate. As attested by Figure 1 of [99] or Figure 2 of [100], many other optical modulation formats are available. Therefore, we can naturally further our study by considering other modulation formats for the message.

In this chapter, we consider that the communication system is fixed with the best synchronization quality possible, and we now focus on the message modulation format. We will first research advanced modulation formats and motivate our choice of three for further investigation. We will then determine how to experimentally generate a suitable message in the given modulation formats before seeing how to properly simulate this process. Secondly, we will look at the simulation aspects of the whole system, detailing the method we used and results for a back-to-back configuration and also after transmission over 50 and 10 km fibers.

6.1 Advanced optical modulation formats

6.1.1 Overview

Significant technological advances have enabled increases in the data rates of optical communication systems (up to 40 Gbits/s) with the number of channels greatly increasing as well with WDM technology [15, 31, 33, 40, 80]. This growth has led to the development of novel optical modulation formats, which most often are used to mitigate linear and nonlinear impairments from fiber-optic transmission and to achieve high spectral efficiencies.

In single-mode optical fibers, the optical field has three physical attributes that can be used to carry information:

- intensity,
- phase (which includes frequency), and
- polarization.

Depending on which of these parameters is used for information transport, we can distinguish between intensity, phase, or polarization data modulation formats (DMF). The communication system that we proposed implements an intensity chaos carrier wave as the cryptographic method. As such, only an intensity coded DMF could be properly encrypted by our system. Any frequency modulation would be easily detectable on the transmission line, and the message could then be recovered by simple filtering.

Even with this restriction, the spectrum of available optical modulation formats is quite large. To break all these modulation formats into categories, we will first distinguish between memory-less and with memory formats. The introduction of memory into a modulation format serves to shape the spectrum of the transmitted signal and to improve the tolerance of a modulation format to a specific propagation impairment. The use of memory in modulation is also referred to as line coding [79]. These techniques have been applied with much success to DMFs with more than two symbols, specifically, to correlative coding and pseudo-multilevel modulation. The enlargement of the symbol alphabet is not

done to decrease the symbol rate but to gain additional degrees of freedom allowing for spectrum shaping and transmission impairment resistance. If the assignment of redundant symbols to transmitted bits is data independent, then the DMF belongs to the category of pseudo-multilevel DMFs. If the assignment of symbols depends on the transmitted data information, then the DMF is in the correlative coding category. The most widespread pseudo-multilevel DMF is the carrier-suppressed return-to-zero (CSRZ), where the information is coded on the intensity levels $\{0, 1\}$, but the phase is changed by π regardless of the information data bit. CSRZ's counterpart for the most wide spread partial response DMF is the optical duobinary format. As for CSRZ, the information is conveyed using two levels $\{0, 1\}$, but the π phase shift only occurs for 1-bits, separated by an odd number of 0-bits [99, 100].

Within the memory-less DMFs, we distinguish between binary and multilevel formats. Multilevel amplitude shift keying (M-ASK) is the prime example of intensity modulation multilevel formats. The counterpart for M-ASK in binary is on-off keying (OOK). In essence, the transmitted bits are differentiated by using two different levels with the transmitter typically turned off to represent the 0-bit and on for the 1-bit, hence the name on-off keying. Within this OOK general class, distinctions can be made between chirped and chirp-free DMFs which both can use return-to-zero or non-return-to-zero schemes. Other formats such as vestigial sideband (VSB) and single sideband (SSB) complete the binary memory-less intensity modulation formats (Figure 1 of [99, 100]).

6.1.2 Modulation format choice

The current research in digital optical communication focuses on two aspects: electronic signal procession (at 10 Gb/s data rates) [30, 53, 68, 72] and modulation formats to mitigate linear and nonlinear impairments inherent to fiber-optic transmission with a 40 Gb/s data rate in mind. To this end, modulation formats have evolved to produce narrower and narrower spectral widths to produce more spectrally efficient signals (from 0.025 bit/s/Hz up to 0.4 bit/s/Hz and beyond) as WDM systems become more and more dense.

Table 4 of [99] lists advanced modulation formats and their required optical signal-to-noise ratio (OSNR) in a back-to-back configuration to reach a BER of 10^{-3}. The authors of [99] warn that the numbers listed can vary because of hardware implementation aspects such as filter characteristics [98] and modulator extinction ratio [76]. For example, Winzer and Essiambre assumed a modulator extinction ratio of 16 dB in the calculation, whereas the ones we used have an extinction ratio of at least 20 dB (Section 3.2.1). Yet, keeping this variation in mind, some general facts are drawn. Of particular importance to us, RZ formats are noted to require in general $1 - 3$ dB less of OSNR than their NRZ equivalents to achieve the same BER [14, 45, 101]. The difference is even greater after transmission over significantly long fibers, more than 6 dB for the RZ-DPSK (differential phase shift keying). Because the optical detection we use only recovers signal intensity, we are limited to intensity modulation schemes, leaving us with the NRZ, RZ and CSRZ on-off keying formats. Even though we are not going to build the corresponding transmitter and receiver for the different message modulation formats, the practical considerations are not far from our minds. In these three modulation formats, the receiver only requires a single photodiode. The transmitter only requires one or two Mach-Zehnder modulators for an optical implementation.

There is another consideration regarding CSRZ67 DMF. When looking at Figure 43, we see the carrier envelope clearly in the middle of the pulse, and the pulse broadening due to modulation as the system behaves more and more chaotically. It may be attributed to the CSRZ format, that part of the optical spectrum could be absent, making the transmitted optical spectrum signature even more neutral.

6.1.3 Message generation methods

First, let us consider the physical implementation of the NRZ, RZ and CSRZ formats.

6.1.3.1 Physically

NRZ-OOK: The simplest DMF to generate is the non-return-to-zero on-off-keying format, usually referred to as NRZ. An electronic binary data stream composed of zeros and ones is naturally in NRZ format. Conversion to an optical data stream can easily be achieved using a directly modulated laser diode, such as the NEL diode NLK5CE2KA of Section 3.2.1. At high bit rates, or for long-haul applications, a Mach-Zehnder modulator (MZM) is preferred. The modulator is biased at the 50% transmission point and is driven from minimum to maximum transmission by a voltage swing of V_π at the data rate.

50 % RZ- OOK: RZ-OOK transmitters can be implemented in multiple ways. The RZ waveform can be generated either electronically and intensity modulated onto an optical carrier using an MZM or a direct-modulated laser diode in the same manner as for NRZ-OOK, as we did in Chapter 4, or by carving pulses out of an NRZ signal using an additional modulator called a pulse carver. As soon as we reach the 10Gb/s mark, the first solution is not feasible anymore and a pulse carver has to be used.

Pulse carving is done by sinusoidally driving an MZM at the data rate between minimum and maximum transmission levels as shown in Figure 78, resulting in pulses with a full-width at half-maximum (FWHM) of 50% of the bit duration.

33 % RZ- OOK: The same method with slightly different settings is used to generate 33% duty cycle pulses. The pulse carver is still present, but this time, the pulse carver modulator bias point is set at a transmission maximum. The drive voltage amplitude is $2 * V_\pi$ at half the data rate. This way, 33% duty cycle pulses are achieved (Figure 78).

67 % CSRZ- OOK: CSRZ is a pseudo-multilevel modulation format [97], characterized by reversing the sign of the optical field at each bit transition. Since the optical field transfer function of the MZM changes sign at the transmission minimum, phase inversions between adjacent bits are produced. Thus, the optical field of half the 1-bits is positive and the other half negative, resulting in a zero-mean field envelope. Therefore, the carrier at the optical center vanishes. This DMF is generated by sinusoidally driving an MZM pulse

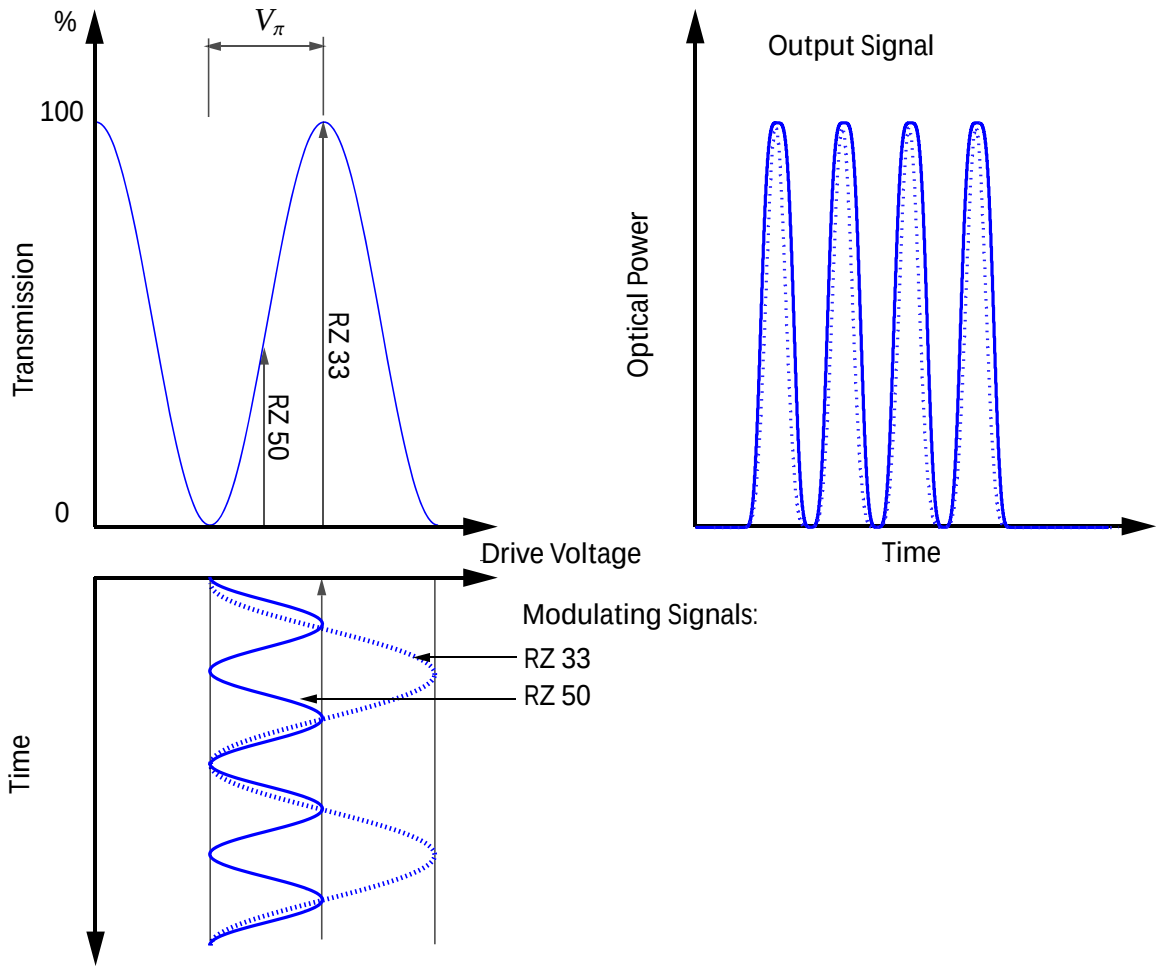


Figure 78: Return-to-zero generation.

carver at half the data rate between two transmission peaks, hence with a bias point at the transmission minimum. This method gives pulses with a 67% duty cycle. Figure 79 shows the optical power (solid line) and the field (dotted line) transmission curves as well as the modulation signal and the CSRZ output signal.

6.1.3.2 In simulation

From a simulation perspective, recreating these different pulses is much easier. The modulator transfer function is a simple sinusoid, as we have seen in Chapter 3 with Equation (25). The variable $V(t)$ represents the drive voltage to the modulator, and ϕ is a function of the bias voltage V_b which sets the operating point of the modulator. Setting $V(t)$ as a sinusoid

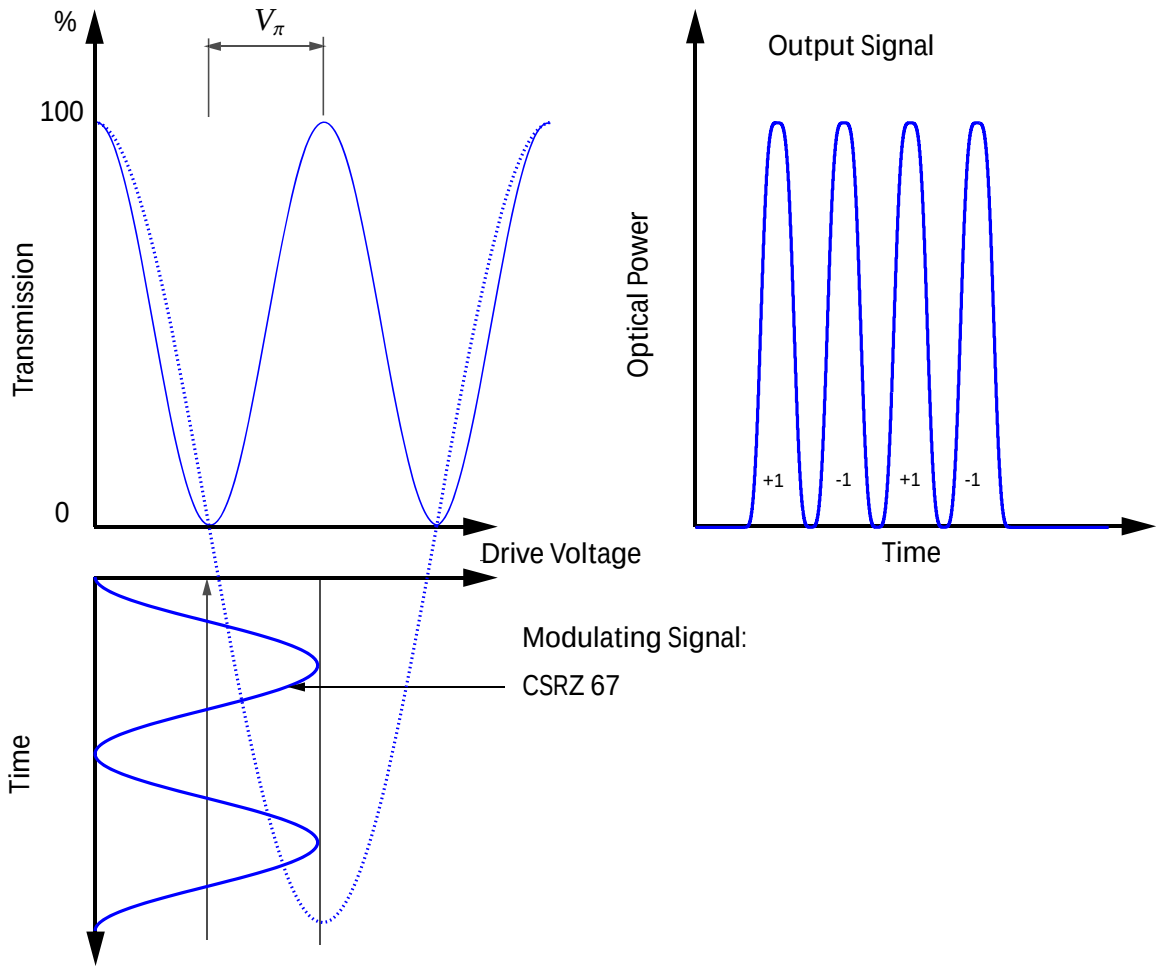


Figure 79: Carrier suppressed return-to-zero generation.

of appropriate frequency and amplitude and properly controlling the phase term ϕ generates different pulsed outputs. The appropriate settings per DMF are detailed in Table 5. As a result, the pulse sequences at 3 Gb/s of Figure 80 are obtained.

Table 5: Appropriate settings for different data modulation formats.

DMF	Amplitude	Frequency	Phase ϕ
RZ 33	$2V_\pi$	3 GHz	0
RZ 50	V_π	1.5 GHz	$\frac{\pi}{2}$
CSRZ 67	$2V_\pi$	3 GHz	π

We have seen how the different DMFs are simulated. We now need to simulate the rest of the chaotic emitter and the corresponding receiver.

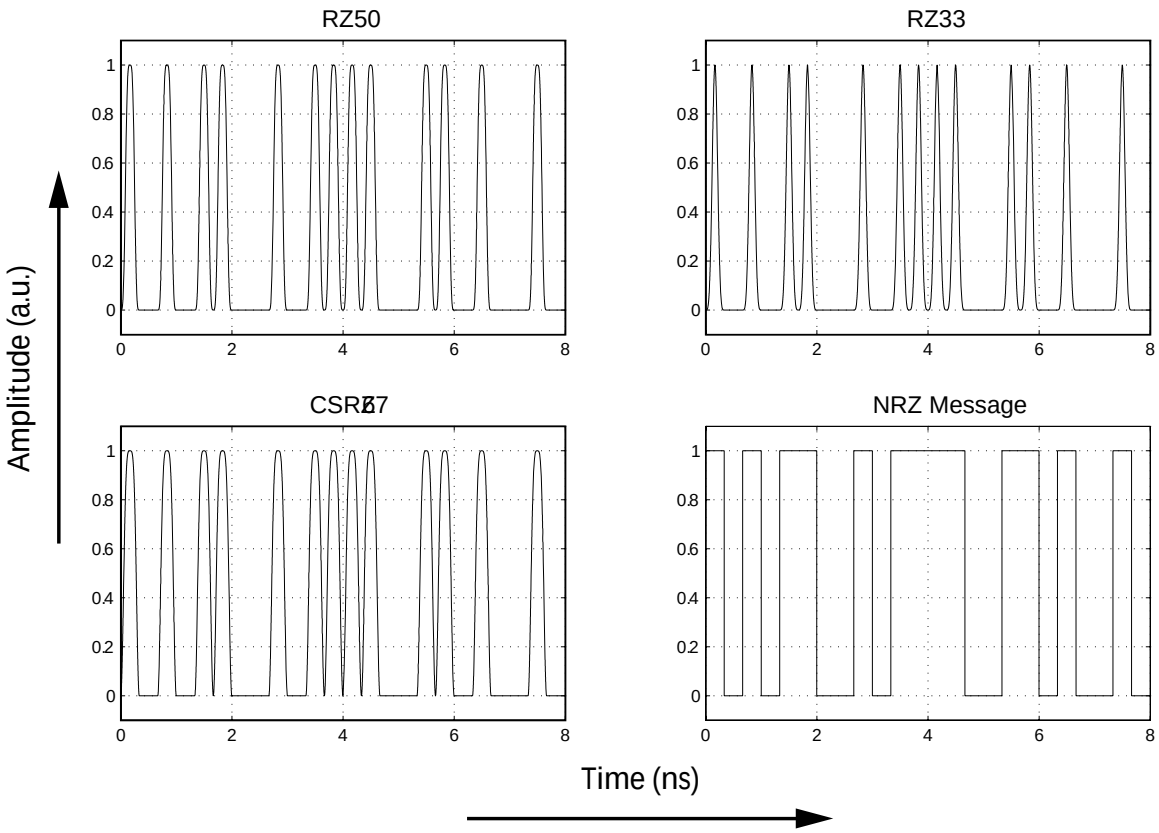


Figure 80: Simulated messages for the different data modulation formats.

6.2 Simulation aspects

The equations modeling the emitter and the receiver are, respectively, Equations (29) and (34). We recall these equations from Chapters 3 and 4.

Emitter:

$$x(t) + \tau \frac{d}{dt} x(t) + \frac{1}{\theta} \int x(t)\, dt = A \left[\cos^2[x(t - T) + \phi] + \alpha\, m(t) \right].$$

Receiver:

$$y(t) + \tau' \frac{dy}{dt}(t) + \frac{1}{\theta'} \int_{t_0}^{t} y(\xi)\, d\xi = \beta' \left[\cos^2(x(t - T) + \phi) + \alpha\, m(t) \right].$$

These are 2^{nd} order delay differential equations for which no analytical solution exists. Therefore, they have to be integrated numerically. Popular methods of numerical integration include predictor-corrector and Runge-Kutta methods [78].

6.2.1 Runge-Kutta method

The Runge-Kutta method is an expansion on the Euler formula:

$$p_{n+1} = q_n + h f(p_n, q_n). \tag{64}$$

The variables p and q have been substituted for the more commonly found x and y variables [26, 43, 78] because those variables have been used to designate the emitter and receiver observables throughout this dissertation.

The Euler formula (64) advances the solution to the differential equation through an interval h but uses derivative information denoted by the function f only at the beginning of that interval. More advanced methods make use of this information at different points in the step interval. A parallel could be drawn between Runge-Kutta methods and series expansions for functions.

Since Equation (29) is 2^{nd} order, to use a Runge-Kutta method, the equation must be split it into two 1^{st} order equations. A simple change of variables is to use $xx(t) = \frac{d\,x(t)}{dt}$, giving us two coupled 1^{st} order equations that will be integrated step-by-step simultaneously. The method we implemented is Verner's method which is a 6th order, 8 stage, explicit Runge-Kutta method [43].

This calculation is done with the following equations [26]:

$$k_1 = f(p_i, q_i), \tag{65}$$

$$k_r = f\left(p_i + c_r h, q_i + h \sum_{j=1}^{r-1} a_{rj} k_j\right), 2 \le r \le 8, \tag{66}$$

$$q_{i+1} = q_i + h \sum_{r=1}^{s} b_r k_r. \tag{67}$$

The a_{rj}, b_r and c_r coefficients are given in the following tables:

In our simulations, we compute $5 \cdot 10^6$ points with a step size of $h = 2 \cdot 10^{-13}$ for a total simulated time of 100 ns. The total simulation time of one 100 ns time period with these

Table 6: Runge-Kutta a_{rj} coefficients.

a_{rj}	1	2	3	4	5	6	7
2	1/6						
3	4/75	16/75					
4	5/6	-8/3	5/2				
5	-165/64	55/6	-425/64	85/96			
6	12/5	-8	4015/612	-11/36	88/255		
7	-8263/15000	124/75	-643/680	-81/250	2484/10625	0	
8	3501/1720	-300/43	297275/52632	-319/2322	24068/84065	0	3850/26703

Table 7: Runge-Kutta b_r coefficients.

b_r	1	2	3	4	5	6	7	8
	3/40	0	875/2244	23/72	264/1955	0	125/11592	43/616

settings takes roughly 40 minutes on an Intel Core 2 Duo PC. With these time traces, we can investigate the behavior of the experimental system of Chapters 3 and 4.

6.2.2 Back-to-back communication

The first setup we investigate to determine system performance for difference message modulation formats is the back-to-back scheme, where the emitter and the receiver of the chaotic communication system are connected by a short fiber optic cable (a couple meters at most). In this situation, all the propagation effects usually experienced in fiber propagation are negligible, therefore DMF propagation robustness is not a factor here. To give a perspective, fiber attenuation is on the order of 0.2 dB/km. Over a meter transmission, this attenuation is 0.0002 dB. As we have seen in Chapter 3, fiber coupling losses are roughly 0.3 dB, three orders of magnitude greater. We anticipate that communication quality is linked to the amount of energy of a ‘1’ bit, a combination of pulse amplitude and pulse width.

In evaluating the system performance, the metric employed is the bit error ratio (BER)

Table 8: Runge-Kutta c_r coefficients.

c_r	1	2	3	4	5	6	7	8
	0	1/6	4/15	2/3	5/6	1	1/15	1

as given by the following equation:

$$BER(D) = \frac{1}{2}\,\mathrm{erfc}\left(\frac{|\mu_1 - D|}{\sigma_1}\right) + \frac{1}{2}\,\mathrm{erfc}\left(\frac{|\mu_0 - D|}{\sigma_0}\right), \tag{68}$$

where D is the voltage decision level, μ_1 the average of the detected values that are considered "ones", σ_1 their standard deviation, and μ_0 and σ_0 are the same for the "zeros". Equation (68) assumes that both the "ones" and the "zeros" in the detected signal have a Gaussian distribution. This formula assumes that the data point measurement is taken at the point where the eye is the most open, to provide the greatest separation between the '1' and the '0' level.

To test to see if observed dada matches a normal distribution, there are several tests available. Common tests are the Kolmogorov-Smirnov, the Lilliefors and the Bera-Jarque tests [42]. We tested the normality of the message distribution with the Bera-Jarque and the Lilliefors test. These tests perform the Lilliefors modification of the Kolmogorov-Smirnov test or the Bera-Jarque test respectively, to determine if the null hypothesis of composite normality is a reasonable assumption regarding the sample set. The desired significance level is set to 0.05. The output of this test, as implemented in Matlab, is binary. If '0', then we do not reject the null hypothesis that the sample is normally distributed at the 0.05 significance level. If the output is '1', then we reject the hypothesis at the significance level.

For different message amplitudes and with three message modulation formats, these tests were performed with the following results (Tables 9 and 10). The message amplitude ranged from 0.025 to 1 for the RZ33, RZ50 and CSRZ67 modulation formats.

According to the Bera-Jarque test, all the decoded messages have a Gaussian distribution. The contrast with the Lilliefors test results for the same 0.05 significance level is clear. Half of the normal distribution hypotheses are rejected according to this test. There also is no discernable pattern for the rejections as seen in Table 10. Since standard normality tests give mitigated results that do not contradict our Gaussian distribution assumption, we feel Equation (68) is applicable.

Table 9: The Bera-Jarque test results.

Amplitude	RZ33 ’0’	RZ33 ’1’	RZ50 ’0’	RZ50 ’1’	CSRZ67 ’0’	CSRZ67 ’1’
0.025	0	0	0	0	0	0
0.05	0	0	0	0	0	0
0.1	0	0	0	0	0	0
0.25	0	0	0	0	0	0
0.5	0	0	0	0	0	0
1	0	0	0	0	0	0

Table 10: The Lilliefors test results.

Amplitude	RZ33 ’0’	RZ33 ’1’	RZ50 ’0’	RZ50 ’1’	CSRZ67 ’0’	CSRZ67 ’1’
0.025	1	1	0	1	0	0
0.05	0	1	0	0	1	0
0.1	1	0	1	1	0	1
0.25	0	0	1	1	0	0
0.5	0	0	0	0	0	0
1	1	0	0	1	1	1

Figure 81 shows an example of the message amplitude distribution. The normalized histogram is plotted (dots) as a function of the message recorded amplitude. The Gaussian distribution is also plotted (solid line) using the mean and standard deviation computed from the groups of "ones" and "zeros".

At this point, we have a simulation that provides us with time series for the emitter and the receiver. Any transmitted message is also recovered and from this data, we can compute the BER, and hence, measure the communication quality. We introduced parameter mismatch to the simulation in keeping with the experimental results of Chapter 4 (Figures 51, 52 and 53). The band-pass filter constants were set to a 1% difference. Similarly, the other parameters (gain, delay, phase) were each subject to a 1% difference. These mismatches were arbitrarily selected with the objective of forcing decryption errors while still being close to the perfectly matched parameter value.

The bit error ratio is computed for each modulation format, for different message amplitudes, with a PRBS7 message. This specific simulation has a certain degree of parameter mismatch, as described above, but without any noise added in the simulation. Figure 82

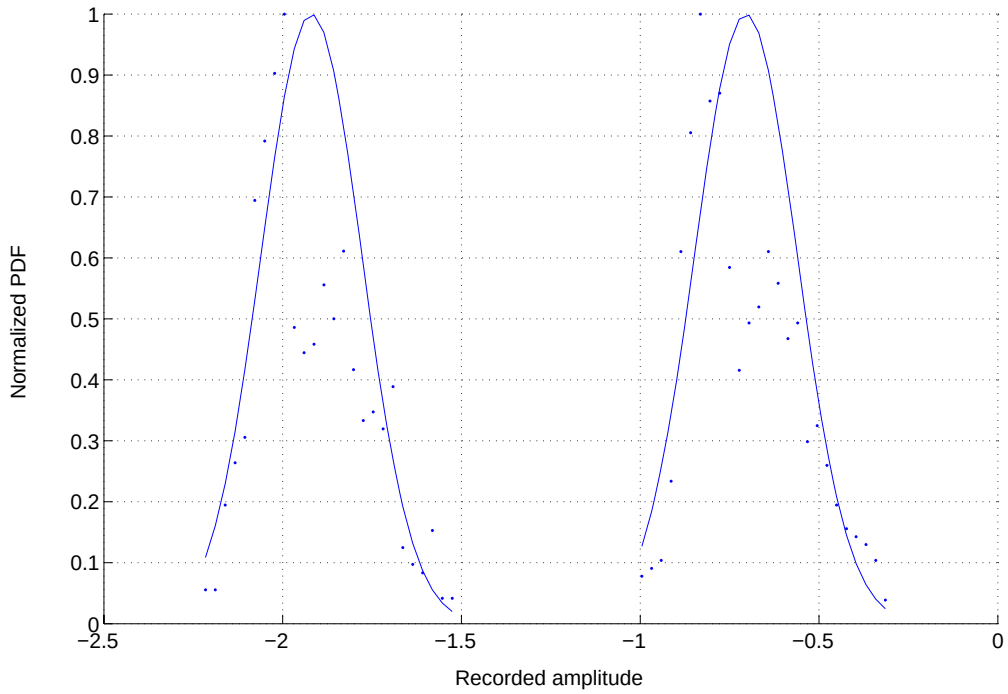


Figure 81: Typical message probability distribution as a function of recorded amplitude.

plots the BER as a function of message amplitude for the RZ33, RZ50 and CSRZ67 message modulation formats. The BER is computed with Equation (68). Care was taken to set the timing of the decision taking when the "ones" were at their maximum detected amplitude in order to maximize the level separation. As observed experimentally, the plots of Figure 82 show a BER that decreases (i.e. higher communications quality), as the message amplitude increases, which was anticipated. What was not anticipated is the separation between the different modulation formats. In the simulation, they all have the same peak amplitude, and since Equation (68) is only dependent on the amplitudes of the data points and not their timing. Since there is no phase jitter built into the simulation, the timing of the decision making should not differentiate between DMFs, at least in the simulation. From an experimental perspective, such results are explainable, as a wider eye opening makes for a smaller (i.e. better) BER.

In the experimental plots of Chapter 4, the RMS value of the message was used for

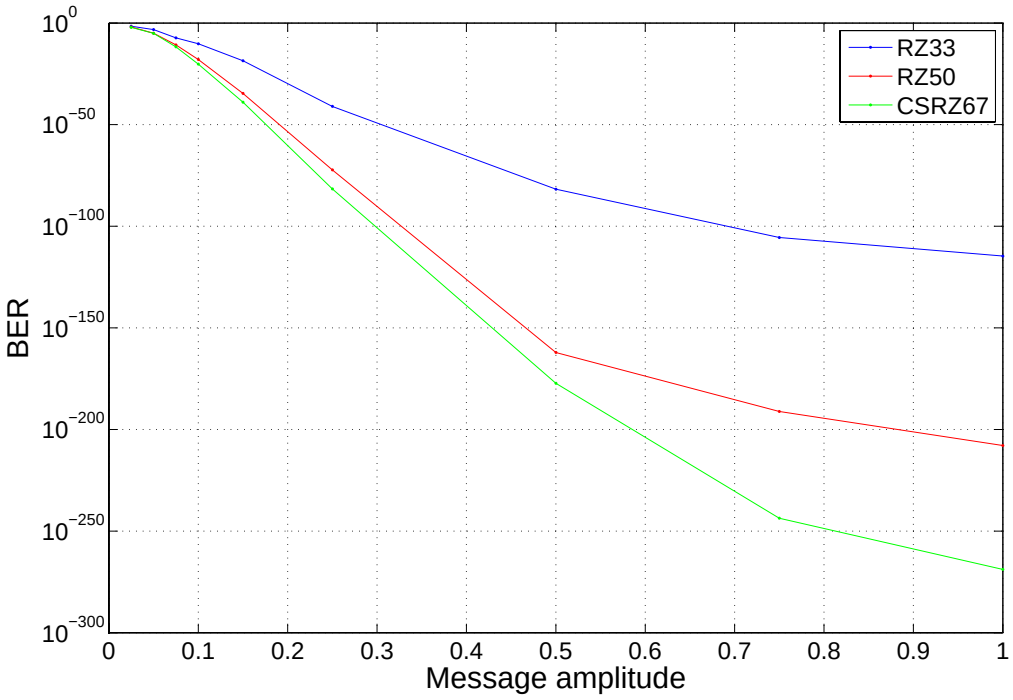


Figure 82: BER plots.

the measure of amplitude, and the chaos RMS value was constant. The RMS value of the message takes into account amplitude as well as duty cycle. Since the messages we are using have a similar shape, and the BER are recorded for given amplitudes, the RMS value gives us a measure that enables for a comparison taking into account the message duty cycle (i.e. the width of the pulses). Also, in basic detection theory, signals with more energy generally feature a lower BER. By comparing performance for equal RMS, we are providing a fair comparison in terms of signal energy. The plot of the BER as a function of message RMS value is found in Figure 83. The RZ50 and CSRZ67 plots are close, until the message RMS value reaches 0.25. The RZ50 BER plot levels out while the CSRZ67 BER plots keeps decreasing before leveling out.

A word of caution should be had when using the RMS value to compare BER plots. Since the width of the RZ33 pulses is shorter than that of its RZ50 and CSRZ67 counter-parts, we were tempted to increase the pulse peak value to match RMS values. While this

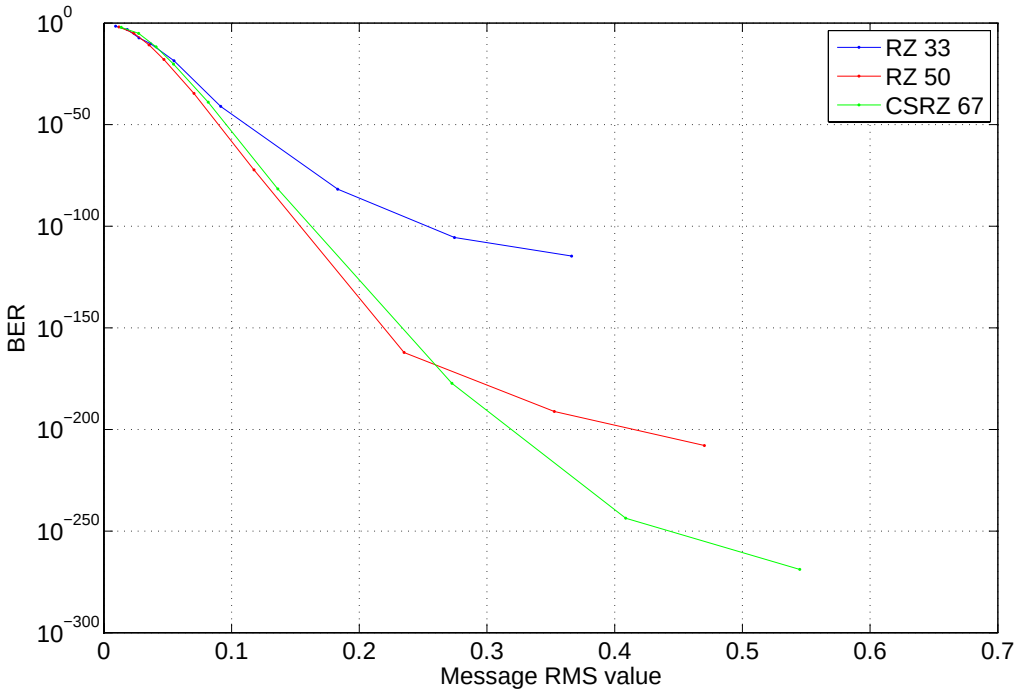


Figure 83: BER plot as a function of message RMS value.

approach could work from a communications quality view point, increasing peak amplitude might be disastrous for the communication security aspect of our system. The message peak value relative to the chaotic carrier amplitude determines if the message is going to appear above the chaotic "noise" during transmission. Past a certain amplitude relative to the chaos level, the message peaks will stand out in the transmitted signal. An unauthorized decryption is then very easily achievable by using a threshold comparison to extract the message peaks. To provide the RMS comparison, the corresponding RMS values were computed for the message magnitude values. This ensures that the message amplitude remains below the security threshold while providing a fair communication quality comparison in terms of message energy.

By looking at Figures 82 and 83, we can see that for lower message amplitude values (≤ 0.5), the RZ50 and CSRZ67 performance are close. Only past this 0.5 mark are the two DMFs differentiable. On the other hand, the RZ33 performance is much worse than the

other DMFs. Therefore, we focus more closely on the RZ50 and CSRZ67 formats, in a effort to accentuate any differences between the two.

To take a slightly different approach in measuring the communication quality, we looked at the evolution of the BER with increasing noise levels in the system. To simulate this effect, a Gaussian white noise was added to the system using the Matlab *randn* function and scaling for the specified noise power σ_n ($noise = \sigma_n * randn$).

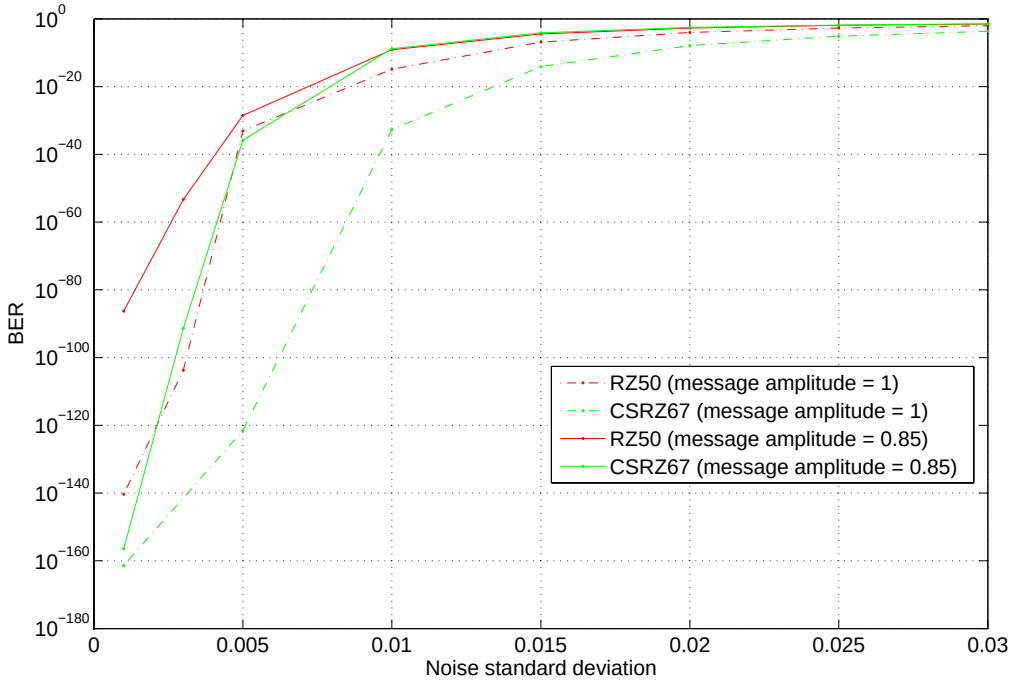


Figure 84: BER as a function of noise standard deviation for fixed message amplitudes 1 (dashed) and 0.85 (solid).

We then proceeded to plot the BER as a function of noise standard deviation σ_n for the RZ50 and CSRZ67 formats with two different message maximum amplitudes: 0.85 and 1 (Figure 84). The RZ50 plots are shown in red and the CSRZ67 in green. The 0.85 amplitude plots are the solid curves, and the 1 amplitudes are dashed. These four curves follow a similar pattern: when the noise power is low, the BER is also very low, with a good communication quality. Then, as the noise level rises, the BER also rises sharply before starting to level out when the noise standard deviation gets in the 0.005 to 0.01

range. The CSRZ67 format consistently exhibits a lower BER than the RZ50 format for both message amplitudes. This difference is particularly important with the 1 message for a noise standard deviation in the range of 0.005 to 0.01, which is the region where the BER transitions from the low noise-low BER combination to high noise-high BER. For the 0.85 message, the separation between the different DMF curves is not as significant.

At the end of this series of simulations involving the RZ33, RZ50 and CSRZ67 data modulation formats in the back-to-back configuration, we conclude that the CSRZ67 DMF achieves better performance as attested by the BER computations. The RZ50 comes in second with RZ33 trailing behind.

While the back-to-back communication quality has been investigated extensively throughout Chapter 4, this analysis is only the first step towards a more realistic scenario involving propagation of the ciphertext through fiber.

6.2.3 Transmission

The need to investigate signal transmission over long fibers is fairly obvious to more closely model likely scenarios for secure communication. Experimental testing has been done both in a laboratory setting (Section 5.1.1) and on deployed fiber [11]. In both cases, the message was the standard NRZ modulation format. In keeping with the nature of this chapter, we depart from this DMF and explore the performance of the RZ33, RZ50 and CSRZ67 data modulation formats.

6.2.3.1 Fiber propagation effects

The phenomenon known as total internal reflection, known since 1854 [89], is responsible for guiding light in optical fibers. Fibers made of glass were made in the 1920s, but with the cladding only appearing in the 1950s. Before 1970, fibers were primarily used for medical imaging over very short distances because of the high losses they exhibited ($\approx$ 1000 db/km). This limitation changed drastically in 1970 when the losses of optical fibers were reduced to a level below 20 db/km [50]. Further research in 1979 resulted in fiber losses of only 0.2

db/km near the 1.55 μm spectral region [69]. Long distance fiber communication was then feasible. Yet, many phenomena still exist that do not make this process easy. The first of these phenomenons was mentioned without being named: attenuation.

Attenuation Several factors impact the attenuation of optical fiber:

- The intrinsic absorption of silica: UV and IR vibrational resonances do not absorb much between 0.2 and 2 μm, but residual impurities can lead to non-negligible absorption levels. In particular, OH ions give the typical attenuation curve of fiber with the two peaks at 1.23 and 1.4 μm. More recent optical fibers did away with this constraint, with attenuation below 0.5 dB/km from 1.26 to 1.62 μm.

- Rayleigh scattering: coming from the local variation of the refraction index, this effect, proportional to λ^{-4}, is dominant at shorter wavelengths and scatters the light in all directions.

The equation relating the optical power measured at a distance z from the source and the power initially injected into the fiber defines the linear attenuation a of the fiber:

$$P(z) = P(0) \cdot e^{-az} \tag{69}$$

with a usually expressed in dB/km according to:

$$a_{dB} = -\frac{10}{z} \log\left(\frac{P(z)}{P(0)}\right) = \frac{10}{\ln 10} a. \tag{70}$$

Chromatic dispersion The response of a dielectric medium to an electro-magnetic wave depends on the wave's frequency ω. The medium is said to be dispersive when its refraction index varies with wavelength. This property plays a crucial role in modern telecommunication, affecting the propagation of short optical pulses as their different spectral components travel at different speeds[1] $\frac{c}{n(\lambda)}$, thus modifying their initial profile in the time domain. The resulting pulse broadening induces inter symbol interferences that limit

[1] The speed of light in vacuum is denoted c.

the total reach of a communication system. For chaos communication, which is by nature of very broad spectrum, this spreading is clearly a concern.

For a quasi-monochromatic wave centered at pulsation ω_0, the dispersion effects are mathematically expressed by expanding the wave vector $\beta(\omega)$ around ω_0:

$$\beta(\omega) = n(\omega)\frac{\omega}{c} = \beta_0 + \beta_1(\omega - \omega_0) + \frac{1}{2}\beta_2(\omega - \omega_0)^2 + \frac{1}{6}(\omega - \omega_0)^3 + \ldots, \qquad (71)$$

where $\beta_i = \frac{d^i\beta}{d\omega^i}\Big|_{\omega=\omega_0}$.

The pulse envelope propagates at group velocity $v_g = \frac{1}{\beta_1}$, where β_2 represents the dispersion of this group velocity. Chromatic dispersion is often expressed by way of the dispersion parameter $D = \frac{d\beta_1}{d\lambda}$:

$$D = \frac{d\beta_1}{d\lambda} = -\frac{2\pi c}{\lambda^2}\beta_2. \qquad (72)$$

The parameter D is usually expressed in $ps/(nm.km)$ and β_2 in ps^2/km. Depending on the sign of D, the dispersion is said to be normal ($D \leq 0$ or $\beta_2 \geq 0$) - the red wavelengths are traveling faster than the blue ones - or anormal ($D \geq 0$). Single mode fibers (SMF), such as the one we used, have zero dispersion around 1.31 μm, which is not the case in the 1.55 μm window where the attenuation is minimum. Other types of fibers have had their characteristics modified and present a different dispersion profile. Among the existing fibers are dispersion shifted fiber (DSF), dispersion flattened fiber (DFF) and, of special interest to us, dispersion compensated fiber (DCF). DCF was used experimentally to correct for the dispersion encountered in the SMF fiber during transmission (Section 5.1.1). Characteristics of the SMF and DCF fibers used were given in Tables 3 and 4.

Non-linear effects Many more effects occur as high power light travels through fiber. These effects are designated here under the general term of non-linear effects. They include self phase modulation (SPM), cross phase modulation (XPM), four wave mixing (FWM) and polarization mode dispersion (PMD). Since these phenomena are not the main subject of this dissertation, we refer the curious reader to the authoritative text on the subject [4].

Non linear Schrödinger equation The governing equation for electric field envelope propagation is derived from the dispersion equation $k = \frac{n\omega}{c}$. After manipulation, we arrive at the propagation equation in the form of the non-linear Shrödinger equation [4]:

$$\frac{\partial F}{\partial z} + \frac{i}{2}\beta_2 \frac{\partial^2 F}{\partial t^2} - i\gamma |F|^2 F = 0, \tag{73}$$

where F is the slowly varying complex envelope of the electric field,[2] $\gamma = \frac{n_2 \omega}{S_{eff} c}$, and S_{eff} is the fiber's effective mode area.

Equation (73) takes into account the dispersion and the SPM effects, but implicitly assumes a lossless propagation medium, which is clearly not the case for propagation through fiber. To correct for this assumption, a generalized Schrödinger equation is defined, including the effects of optical amplification (gain $g(z)$, noise $\hat{F}(z,t)$), the third order dispersion β_3 and the optical filtering (filter factor $b(z)$).

$$i\frac{\partial F}{\partial z} - \frac{1}{2}[\beta_2(z) - ib(z)] \cdot \frac{\partial^2 F}{\partial t^2} + \frac{\beta_3}{6}\frac{\partial^3 F}{\partial t^3} + \gamma(z)|F|^2 F = ig(z)u + \hat{F}(z,t) \tag{74}$$

In the literature, a normalization is often introduced:

$$Z = \frac{z}{z_0}, T = \frac{\tau}{\tau_0}, q = \sqrt{\frac{n_2 \omega_1 z_0}{c}} E \text{ and } z_0 = -\frac{\tau_0^2}{k_0''}, \tag{75}$$

which leads to the more condensed form of the NLSE:

$$j\frac{\partial q}{\partial Z} + \frac{1}{2}\frac{\partial^2 q}{\partial T^2} + |q|^2 q = 0. \tag{76}$$

6.2.3.2 Simulation method

The NLSE (76) is a nonlinear partial differential equation that presents analytic solutions for specific cases where the inverse scattering method can be employed. However, this solution is not applicable in most cases. Frequently used in the literature [4], the split-step Fourier method considers the two major transmission impairments, the SPM and the dispersion, as independent over an elementary distance dz. So Equation (73) is solved separately, considering only the chromatic dispersion ($\frac{\partial F}{\partial z} + \frac{i}{2}\beta_2 \frac{\partial^2 F}{\partial t^2} = 0$), and then only the Kerr effect

[2] A is usually used in the literature.

($\frac{\partial F}{\partial z} - i\gamma|F|^2F = 0$). These two equations are analytically solved in the frequency domain and the time domain, respectively, for the dispersive and the nonlinear parts. From a mathematical perspective, this approach is equivalent to computing the limited development (i.e. as $h \to 0$) of the exact solution:

$$F(z+h,T) = e^{h(\hat{D}+\hat{N})}F(z,T) \tag{77}$$

of the NLSE expressed in the following form:

$$\frac{\partial F}{\partial z} = (\hat{D}+\hat{N})F, \tag{78}$$

where $\hat{D}$ and $\hat{N}$ are the differential operators for dispersion and nonlinearity

$$\hat{D} = -\frac{i}{2}\beta_2\frac{\partial^2}{\partial t^2} + \frac{1}{6}\beta_3\frac{\partial^3}{\partial t^3} - \frac{a}{2} \tag{79}$$

$$\hat{N} = i\gamma|F|^2. \tag{80}$$

For two non commutative operators, the Baker-Hausdorf formula is given by:

$$e^{\hat{a}} \cdot e^{\hat{b}} = e^{\hat{a}+\hat{b}+\frac{1}{2}[\hat{a},\hat{b}]+\frac{1}{12}[\hat{a}-\hat{b},[\hat{a},\hat{b}]]+\ldots} \tag{81}$$

with $[\hat{a},\hat{b}] = \hat{a}\hat{b} - \hat{b}\hat{a}$. As a first order approximation, we get $e^{\hat{a}} \cdot e^{\hat{b}} \approx e^{\hat{a}+\hat{b}}$ and the first neglected term is

$$\frac{1}{2}[\hat{a},\hat{b}] = \frac{1}{2}h^2[\hat{D},\hat{N}].$$

This assumption gives the split step Fourier method an accuracy to second order in the step size h. The previous development is used to provide a numerical expression $F(z+h,T)$. The exponential is computed in the Fourier domain according to:

$$e^{h\hat{D}} \cdot B(z,T) = \{\mathscr{F}^{-1}e^{h\hat{D}(i\omega)}\mathscr{F}\}B(z,T). \tag{82}$$

The fast techniques available to compute the Fourier transform, specifically the fast Fourier transform (FFT), make this algorithm faster than other techniques, such as finite differences. In the Fourier domain, the expression for $\hat{D}$ is reduced to the computation of a

complex number with the equivalence $\frac{\partial}{\partial t} \leftrightarrow j\omega$. The accuracy can also be further improved. Instead of computing the nonlinear distortions and then the dispersion effects on the step size h, we can use a symmetric version of the algorithm. We first compute the dispersion effects on $h/2$, then apply the nonlinear effects on the full step h, before computing the dispersion effects on the remaining $h/2$ with:

$$F(z+h,T) \approx e^{\frac{h}{2}\hat{D}} \cdot e^{\hat{N}} \cdot e^{\frac{h}{2}\hat{D}} F(z,T). \tag{83}$$

We will use this algorithm in our work, as the increased precision comes with a low computational overhead.

6.2.3.3 Simulated transmission

The split-step Fourier algorithm for propagation along an optical fiber was implemented in Matlab. The evolution of the envelope of the optical field was recorded after every kilometer of propagation. The propagation line is made of $\approx$ 50 km modules as shown in Figure 61 that are linked according to Figure 62. In our case, we simulate two modules of $\approx$ 50 km to achieve a total transmission of 100 km.

A typical chaotic signal propagation over 100 km is shown in Figure 85. While the distortion and the non-linear effects are hard to see for a propagating chaotic signal, the attenuation of the fiber and the positioning of the erbium doped fiber amplifier (EDFA) at the 50 km mark are very obvious. The 100 km EDFA is not shown in the figure. Less obvious, but also very important, are the short (6 km) spans of dispersion compensated fiber (DCF) that are inserted after the longer spans (50 km) of single mode fiber (SMF). The lengths of the DCF fiber spans were carefully chosen so that the total dispersion of the fiber would be very close to zero at the moment of detection.

The procedure to simulate the transmission is very close to that of the back to back case. The output of the emitter is the same. The time step size remains $3 \cdot 10^{-13}$ seconds. The total simulated time was reduced from 1μs to 0.8μs, because of memory limitations when simulating the propagation and recording the transmitted time points after different

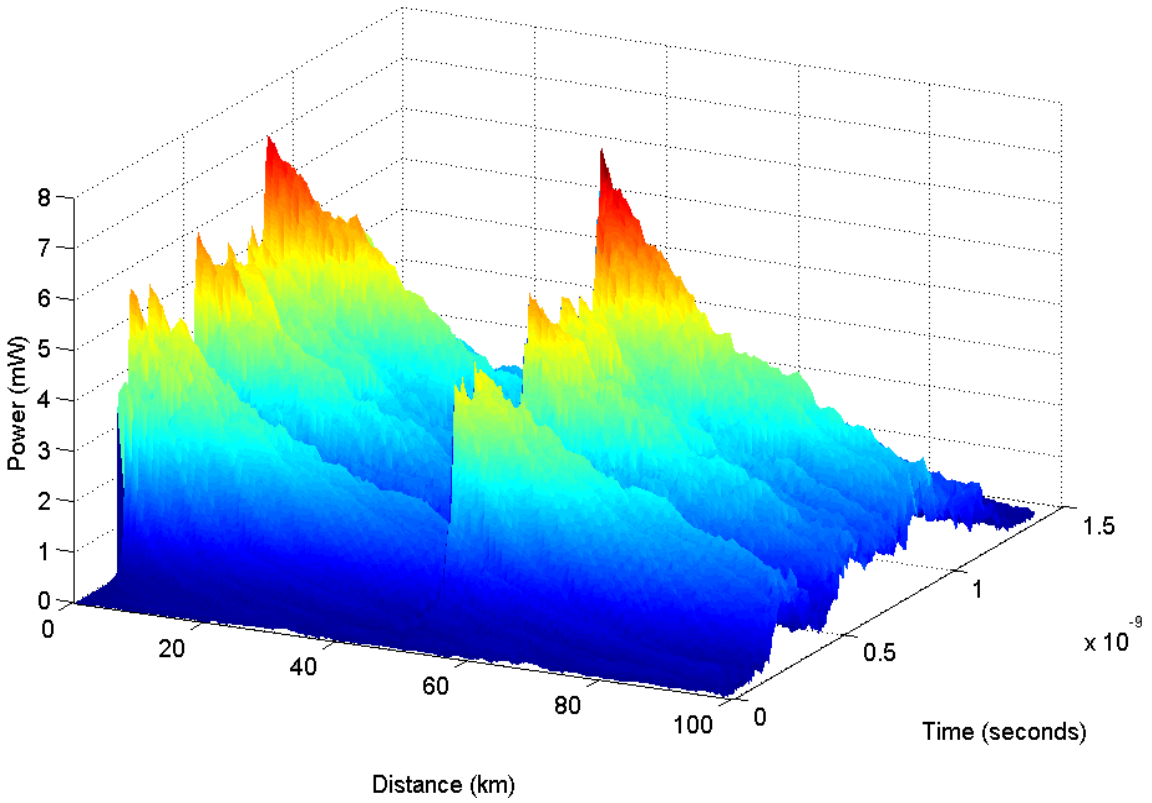


Figure 85: Propagating chaotic signal.

propagation distances. The output of the emitter was run through the propagation program. The time vector resulting from propagation was then input to the receiver for decoding. The decoder output the recovered message. Using Equation (68), we compute the bit error ratio for the communication. The message amplitudes in our simulations range from 0.1 to 0.95 for the three modulation formats we have been using: RZ33, RZ50, and CSRZ67. The BER is plotted as a function of message amplitude after a 50 km transmission in Figure 86. As expected, the BER decreases as the message amplitude increases for all three modulation formats. Also, the transmission does not change the order of performance of the modulation formats. CSRZ67 still displays the best performances, with RZ33 the worst.

The BER is then plotted for the same message amplitude values after a transmission of 100 km in Figure 87. The plots show the same general aspect as those of Figure 86 with the BER values remaining very close. These plots are also comparable to the ones of Figure 82, but higher, indicating a lower communication quality resulting from the propagation over fiber.

Throughout these simulations, whether in back-to-back mode or after propagation, the bit error ratios computed are very low, and hardly obtainable experimentally. Because of the very high precision achieved by the floating point representation, the decoding can be done with high accuracy for very good BERs. Even incorporating noise, parameter mismatch, and propagation in the simulation does not impede synchronization and communication quality, as much as would be the case experimentally. One aspect that was already mentioned in Chapter 5 is the matching of the modulator transfer function shape. Experimentally, little can be done to correct for this distortion, and this mismatch would introduce systematic errors, as soon as the signal sweeps this part of the transfer function. In simulation, both transfer functions are of the exact same $\cos^2$ shape.

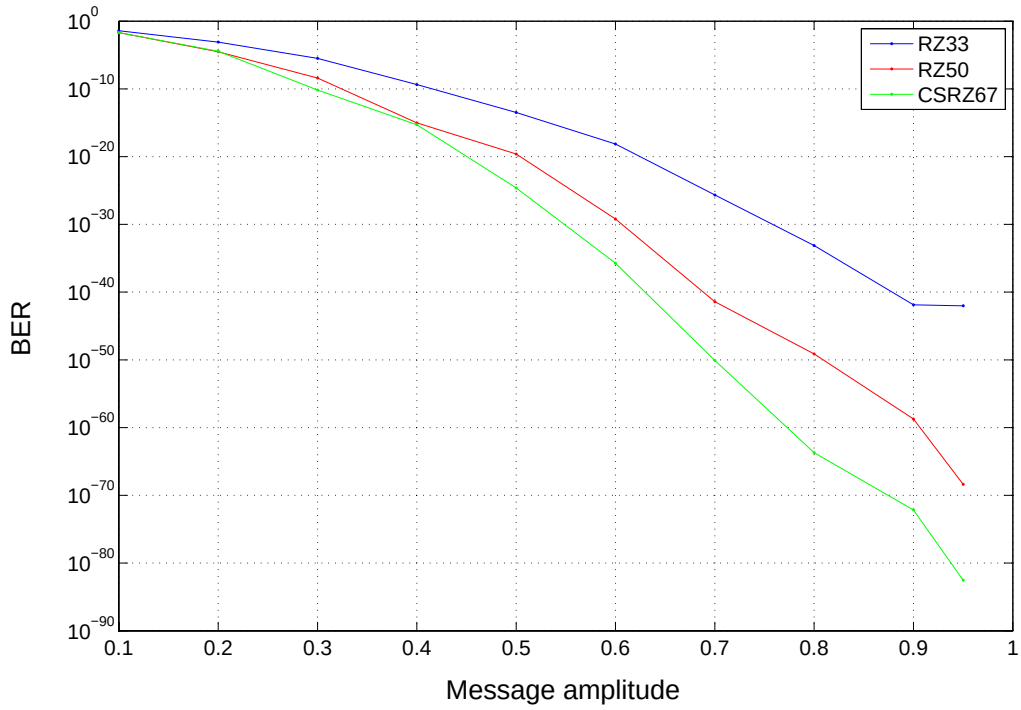


Figure 86: BER evolution as a function of message amplitude after 50 km propagation.

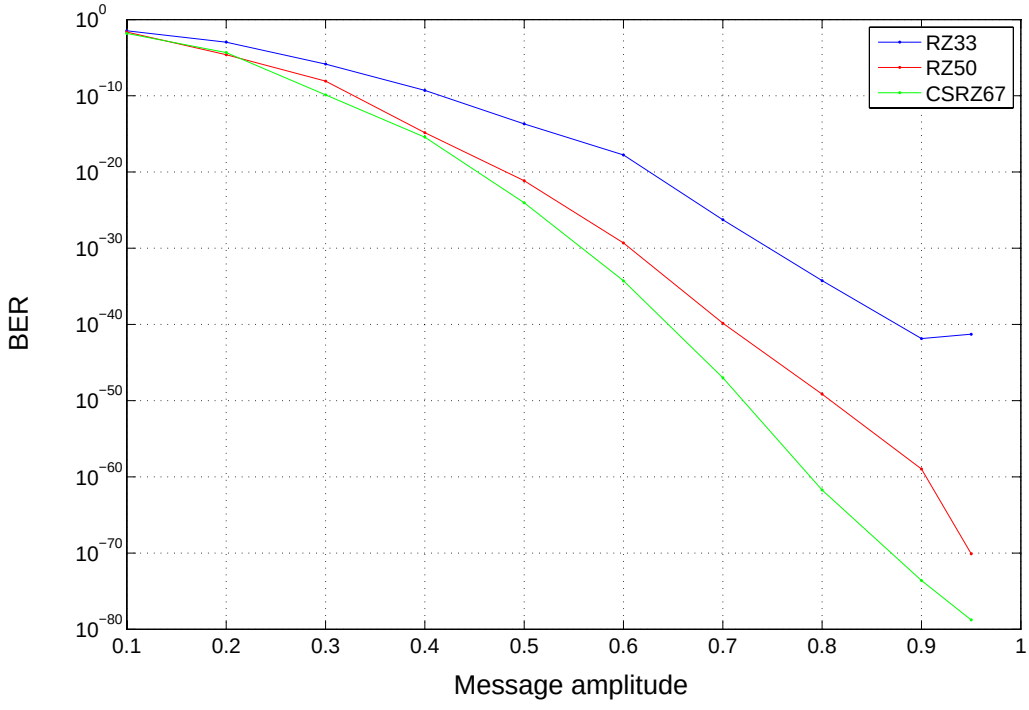


Figure 87: BER evolution as a function of message amplitude after 100 km propagation.

Conclusion

In this chapter, we presented work done to simulate the communication quality as a function of message modulation format and message amplitude. The different message modulation formats used in this study are the return-to-zero format with both 33% and 50% duty cycles (RZ33 and RZ50) and the carrier-suppressed return-to-zero format with a 67% duty cycle (CSRZ67).

The equations modeling the system were numerically integrated using the Runge-Kutta method (Section 6.2.1) in order to compute the bit error ratio (BER) and measure the communication quality. This simulation was first done in the back-to-back configuration (Section 6.2.2). Progressively, parameter mismatch and noise were added to induce errors and to more closely approximate an experimental case. Each time, the BERs were compared for the different message modulation formats, with the CSRZ67 systematically performing better then the two RZ formats.

The last step was to simulate the propagation of the chaotic signal over 50 and 100 km before proceeding to the decoding as had been done in Chapter 5. The method used to simulate propagation was the split-step Fourier method (Section 6.2.3.2). Again, the CSRZ67 modulation format yielded better communication quality than the return-to-zero formats.

CONCLUSION

This thesis was done partly at the GTL-CNRS Telecom lab housed on the campus of Georgia Tech Lorraine, the European platform of Georgia Tech, and at the Center for Signal and Image Processing (CSIP) on the Atlanta campus. Partions of this work were also part of a three-year European Union contract called OCCULT (Optical chaos communication using laser transmitters). The work presented here met or exceeded our contract objectives, which were the development of a gigahertz chaos encryption system.

Contributions

- We demonstrated a chaos generator suitable for Telecom purposes. Its bandwidth is wide enough to provide encryption for modern high-bit-rate signals. We determined the chaotic operating zone of the emitter by constructing the emitter bifurcation diagram and measured the frequency footprint of the system both electronically and optically.

- The construction of the highly-specific receiver matching our chaotic emitter was achieved. The study of its performances and the performances of the complete (emitter and receiver) system underlined the applicability of the system as a whole. We also studied the evolution of the synchronization quality as a function of each experimentally adjustable system parameter before evaluating the communication quality using the bit error ratio (BER) as a metric. This study provided with operation information to achieve optimal system performance. At a 3 Gbit/s rate, the decoded message BER was measured at $7 \cdot 10^{-9}$ while a spy could not directly decrypt the transmitted message.

- The system limitations that we encountered during its implementation were characterized. They are mostly communication quality issues and encryption confidentiality. We proposed modifications with the objective of increasing system quality to

provide stronger encryption.

- The study of the impact of message modulation format on the system performance was presented. Three data modulation formats were compared: RZ33, RZ50 and CSRZ67. Parameter mismatch, noise and both 50 and 100 km propagation were included. It was found that the CSRZ67 format consistently outperformed the two RZ formats.

Future work

- A non-linear physics approach would be to study the chaotic dynamic that is generated. The system we developed is modeled with a second order delay differential equation as opposed to the first order ones that have been used for the other opto-electronic systems. The band-pass nature of the system can bring about positive changes in terms of chaos complexity, hence a confidentiality increase. Further theoretical studies would be needed to confirm the link between the band pass nature of the system and the complexity.

- From a telecom perspective, it would be very interesting to study the integration of the system we developed in a WDM setting, both in simulation and in practice. If synchronization and decoding could be maintained after a carrier wavelength change, chaos cryptography could potentially be integrated and deployed in modern MPλS system.

REFERENCES

[1] *De Bello Gallico - Commentaires sur la Guerre des Gaules*. Flammarion.

[2] "Distributed Feedback (DFB) Lasers," in *Beginner's Guides*, http://www.lightreading.com, August 2001.

[3] Agrawal, G. P., *Fiber-Optic Communication Systems*. Wiley series in microwave and optical engineering, Wiley Interscience, 2nd edition ed., 1997.

[4] Agrawal, G. P., *Nonlinear Fiber Optics*. San Diego : Academic Press, 3rd ed., 1989.

[5] Aida, T. and Davis, P., "Oscillation modes of laser diode pumped hybrid bistable system with large delay and application to dynamical memory," *IEEE J. Quantum Electron.*, vol. 28, pp. 686–699, March 1992.

[6] Andrews, J. R., *Low-Pass Risetime Filters for Time Domain Applications*. Picosecond Pulse Labs, Mars 1999.

[7] Annovazzi-Lodi, V., Donati, S., and Manna, M., "Chaos and locking in a semiconductor laser due to external injection," *IEEE J. Quantum Electron.*, vol. 30, pp. 1537–1541, July 1994.

[8] Annovazzi-Lodi, V., Merlo, S., Norgia, M., and Scirè, A., "Characterization of a chaotic telecommunication laser for different fiber cavity lengths," *IEEE J. Quantum Electron.*, vol. 38, pp. 1171–1177, September 2002.

[9] Annovazzi-Lodi, V., Scirè, A., Sorel, M., and Donati, S., "Dynamic behavior and locking of a semiconductor laser subjected to external injection," *IEEE J. Quantum Electron.*, vol. 34, pp. 2350–2357, December 1998.

[10] ANSI X3.92, "American national standard for data encryption algorithm (DEA)." American National Standard Institute, 1981.

[11] Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I., Garcia-Ojalvo, J., Mirasso, C. R., Pesquera, L., and Shore, K. A., "Chaos-based communication at high bit rates using commercial fibre-optic links," *Nature*, vol. 437, pp. 343–346, November 2005.

[12] Bergé, P., Pomeau, Y., and Vidal, C., *L'Ordre dans le Chaos, vers une Approche Déterministe de la Turbulence*. Hermann, 1988.

[13] Bienfang, J., Gross, A., Mink, A., Hershman, B., Nakassis, A., Tang, X., Lu, R., Su, D., Clark, C. W., Williams, C. J., Hagley, E., and Wen, J., "Quantum key distribution with 1.25 Gbps clock synchronization," *Optics Express*, vol. 12, pp. 2011–2016, May 2004.

[14] Boivin, L. and Pendock, G., "Receiver sensitivity for optically amplified RZ signals with arbitrary duty cycle," in *Proc. Optical Amplifiers and Their Applications (OAA)*, 1999. Paper ThB4.

[15] Charlet, G., Corbel, E., Lazaro, J., Klekamp, A., Dischler, R., Tran, P., Idler, W., Mardoyan, H., Konczykowska, A., Jorge, F., and Bingo, S., "WDM transmission at 6 Tbit/s capacity over transatlantic distance and using 42.7 Gb/s differential phase-shift keying without pulse carver," in *Proc. Optical Communication Conference (OFC)*, 2004. Paper PDP36.

[16] Chembo Kouomou, Y., Colet, P., Gastaud, N., and Larger, L., "Effect of Parameter Mismatch on the Synchronization of Chaotic Semiconductor Lasers with Electrooptical Feedback," *Phys. Rev. E.*, vol. 69, no. 056226, 2004.

[17] Chembo Kouomou, Y., Colet, P., Larger, L., and Gastaud, N., "Mismatch-induced bit error rate in optical chaos communications using semiconductor lasers with electrooptical feedback," *IEEE J. Quantum Electron.*, vol. 41, pp. 156–163, February 2005.

[18] Chua, L., Komuro, M., and Matsumoto, T., "The double scroll family, Parts I and II," *IEEE Trans. Circuits Syst.*, vol. CAS-33, no. 11, pp. 1073–1118, 1986.

[19] Cuenot, J.-B., Larger, L., Goedgebuer, J.-P., and Rhodes, W., "Chaos shift keying with an optoelectronic encryption system using chaos in wavelength," *IEEE J. Quantum Electron.*, vol. 37, no. 7, pp. 849–855, 2001.

[20] Cuenot, J.-B., *Système optoélectronique de communication sécurisé par chaos en longueur d'onde*. PhD thesis, U.F.R des Sciences et Techniques de l'Université de Franche-Comté, Février 2002.

[21] Cuomo, K. M. and Oppenheim, A. V., "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, July 1993.

[22] Cuomo, K. M., Oppenheim, A. V., and Strogatz, S. H., "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 626–633, October 1993.

[23] Daisy, R. and Fischer, B., "Synchronization of chaotic nonlinear optical ring oscillators," *Optics Comm.*, vol. 133, pp. 282–286, January 1997.

[24] Diffie, W. and Hellman, M. E., "Multiuser cryptographic techniques," in *Proceedings of AFIPS National Cmputer Conference*, pp. 109–112, 1976.

[25] Dorizzi, B., Grammaticos, B., Le Berre, M., Pomeau, Y., Ressayre, E., and Tallet, A., "Statistics and dimension of chaos in differential delay systems," *Phys. Rev. A.*, vol. 35, pp. 328–339, January 1987.

[26] Enright, W. H., Higham, D. J., Owren, B., and Sharp, P. W., "A Survey of the Explicit Runge-Kutta Method," Tech. Rep. 94-291, 1994.

[27] ETEBAC, "Echanges télématiques entre les banques et leurs clients." Comité Français d'Organisation et de Normalisation Bancaires, April 1989.

[28] Fischer, I., Hess, O., Elsässer, W., and Göbel, E., "High-dimensional chaotic dynamics of an external cavity semiconductor laser," *Phys. Rev. Lett.*, vol. 73, pp. 2188–2191, October 1994.

[29] Fraser, A. M. and Swiney, H. L., "Independant coordinates for strange attractors from mutual information," *Phys. Rev. A.*, vol. 33, pp. 1134–1140, February 1986.

[30] Färbert, A., Langenback, S., Stojanociv, N., Dorschky, C., Kupfer, T., Schulien, C., Elbers, J.-P., Griesser, H., and Glingener, C., "Performance of a 10.7-Gb/s receiver with digital equalizer using maximum likelihood sequence estimation," in *Eur. Conf. Optical Commun. (ECOC), Stockholm, Sweden*, 2004. Paper Th4.1.5.

[31] Frignac, Y., Charlet, C., Idler, W., Dischler, R., Tran, P., Lanne, S., Martinelli, C., Veith, G., Jourdan, A., Hamaide, J.-P., and Bigo, S., "Transmission of 256 wavelength-division and polarization-division-multiplexed channels at 42.7 Gb/s (10.2 Tb/s capacity) over 3*100 km of TeraLight fiber," in *Proc. Optical Fiber Communication Conf. (OFC)*, 2002. Paper FC5.

[32] Fujisaka, H. and Yamada, T., "Stability theory of synchronized motion in coupled-oscillator systems," *Prog. Theor. Phys.*, vol. 69, pp. 32–47, 1983.

[33] Fukuchi, K., Kasamatsu, T., Morie, M., Ohhira, R., Ita, T., Sekiya, K., Ogasahara, D., and Ono, T., "10.92-Tb/s -(273*40-Gb/s) triple-band/ultra-dense WDM optical-repeatered transmission experiment," in *Proc. Optical Fiber Communication Conf. (OFC)*, 2001. Paper PD24.

[34] Garon, G. and Outerbridge, R., "DES watch : an examination of the sufficiency of the data encryption standard for financial institution security in the 1990's," *Cryptologia*, vol. 15, pp. 177–193, July 1991.

[35] Gastaud, N., Poinsot, S., Larger, L., Merolla, J.-M., Hanna, M., Goedgebuer, J.-P., and Malassenet, F., "Electro-optical chaos for multi-10 Gbit/s optical transmissions," *Electron. Lett.*, vol. 40, pp. 898–899, July 2004.

[36] Genin, E., Larger, L., Goedgebuer, J.-P., Lee, M. W., Ferrière, R., and Bavard, X., "Chaotic oscillations of optical phase for multigigahertz-bandwidth secure communications," *IEEE J. Quantum Electron.*, vol. 40, pp. 294–298, March 2004.

[37] Geodgebuer, J.-P., Larger, L., and Porte, H., "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," *Phys. Rev. Lett.*, vol. 80, pp. 2249–2252, March 1998.

[38] Gleick, J., *La théorie du chaos : vers une nouvelle science*. Champs Flammarion, 1987.

[39] Güémez, J. and Matías, M., "On the synchronization of identically driven chaotic systems," *Phys. Lett. A*, vol. 246, pp. 289–292, September 1998.

[40] Gnauck, A., Raybon, G., Chandrasekhar, S., Leuthold, J., Doerr, L., Agarwal, A., Banerjee, S., Grosz, D., Hunsche, S., Kung, A., Maywar, D., Movassaghi, M., Liu, X., Xu, C., Wei, X., and Gill, D., "2.5 Tb/s (64*42.7 Gb/s) transmission over 40*100 km NZDSF using RZ-DPSK format and all-Raman-amplified spans," in *Proc. Optical Fiber Communication Conf. (OFC)*, 2002. Paper FC2.

[41] Goedgebuer, J.-P., Levy, P., Larger, L., Chen, C.-C., and Rhodes, W. T., "Optical communication with synchronized hyperchaos generated electro-optically," *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1178–1183, 2002.

[42] Gujarati, D. N., *Basic Econometrics*. 4th ed., 2003.

[43] Hairer, E., Norsett, S. P., and Wanner, G., *Solving Ordinary Differential Equations 1: Nonstiff Problems*. Springer-Verlag, 2nd ed., Aug 1993.

[44] Hegger, R., Bünner, M. J., and Kantz, H., "Identifying and modeling delay feedback systems," *Phys. Rev. Lett.*, vol. 81, pp. 558–561, July 1998.

[45] Idler, W., Klelamp, A., Dischler, R., Lazaro, J., and Konczykowska, A., "System performance and tolerances of 43 Gb/s ASK and DPSK modulation formats," in *Proc. Eur. Conf. Optical Communication (ECOC)*, 2003. Paper Th.2.6.3.

[46] Ikeda, K., Daido, H., and Akimoto, O., "Optical turbulence: Chaotic behavior of transmitted light from a ring cavity," *Phys. Rev. Lett.*, vol. 45, pp. 709–712, Sep 1980.

[47] Ikeda, K., Kondo, K., and Akimoto, O., "Successive high-harmonic bifurcations in systems with delayed feedback," *Phys. Rev. Lett.*, vol. 49, pp. 1467–1470, November 1982.

[48] Ikeda, K., "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Optics comm.*, vol. 30, pp. 257–261, August 1979.

[49] Kaminow, I. and Li, T., *Optical Fiber Communication*, vol. IV B. Academic Press, 2002.

[50] Kapron, F., Keck, D. B., and Maurer, R. D., "Radiation losses in glass optical waveguides," *Appl. Phys. Lett.*, vol. 17, no. 10, pp. 423–425, 1970.

[51] Kennedy, M. P., "Three steps to chaos - part I: Evolution," *IEEE Trans. Circuits Syst. I*, vol. 40, pp. 640–656, October 1993.

[52] Kennedy, M. P., "Three steps to chaos - part II: A Chua's circuit primer," *IEEE Trans. Circuits Syst. I*, vol. 40, pp. 657–674, October 1993.

[53] Kikychi, K., "Coherent detection of phase-shirt keying signals using digital carrier-phase estimation," in *Optical Fiber Commun. Conf. (OFC), Anaheim, CA*, 2006. Paper OTuI4.

[54] Kocarev, L., Halle, K., Eckert, K., and Chua, L., "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation and Chaos*, vol. 2, no. 3, pp. 709–713, 1992.

[55] Konnur, R., "Synchronization-based approach for estimating all model parameters of chaotic systems," *Phys. Rev. E.*, vol. 67, p. 027204, 2003.

[56] Lang, R. and Kobayashi, K., "External optical feedback effects on semiconductor injection laser properties," *IEEE J. Quantum Electron.*, vol. 16, pp. 347–355, March 1980.

[57] Larger, L., *Cryptage de signaux par chaos en longueur d'onde*. PhD thesis, U.F.R des Sciences et Techniques de l'Université de Franche-Comté, Janvier 1997.

[58] Larger, L., Goedgebuer, J.-P., and Delorme, F., "Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator," *Phys. Rev. E.*, vol. 57, pp. 6618–6624, June 1998.

[59] Lee, M. W., *Etude des comportements chaotiques en modulation de cohérence et application à la cryptographie*. PhD thesis, U.F.R des Sciences et Techniques de l'Université de Franche-Comté, Février 2002.

[60] Lee, M. W., Larger, L., and Goedgebuer, J.-P., "Transmission System Using Chaotic Delays Between Lightwaves," *IEEE J. Quantum Electron.*, vol. 39, pp. 931–935, July 2003.

[61] Lee, M. W., Larger, L., Oudaltsov, V., Genin, E., and Geodgebuer, J.-P., "Demonstration of a chaos generator with two time delays," *Optics Letters*, vol. 29, pp. 325–327, February 2004.

[62] Levy, P., *Télécommunications Optiques Cryptées par Chaos*. PhD thesis, U.F.R des Sciences et Techniques de l'Université de Franche-Comté, April 2004.

[63] Lin, S. and Costello, D. J., *Error Control Coding : Fundamentals and Applications*. Prentice Hall, October 1982.

[64] Liu, J., "Chaos synchronization in semiconductor lasers," in *Lasers and Electro-Optics Society 1999 12th Annual Meeting*, vol. 1, pp. 377–378, IEEE LEOS, 1999.

[65] Liu, J., Chen, H., and Tang, S., "Optical-communication systems based on chaos in semiconductor lasers," *IEEE Trans. Circuits Syst. I*, vol. 48, pp. 1475–1483, December 2001.

[66] Lorenz, E. N., "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, pp. 130–141, 1963.

[67] Matsumoto, T., "A chaotic attractor from Chua's circuit," *IEEE Trans. Circuits Syst.*, vol. CAS-31, no. 12, pp. 1055–1058, 1984.

[68] McGhan, D., ans A. Savchenko, C. L., Li, C., Mack, G., and O'Sullivan, M., "5120 km RZ-DPSK transmission over g.652 fiber at 10 Gb/s with no optical dispersion compensation," in *Optical Fiber Commun. Conf. (OFC), Anaheim, CA*, 2005. Paper PDP27.

[69] Miya, T., Terunuma, Y., Hosaka, T., and Miyoshita, T., "Ultimate low-loss single-mode fibre at 1.55 m," *Electron. Lett.*, vol. 15, pp. 106–108, February 1979.

[70] Newton, H., *Newton's Telecom Dictionary*. CMPbooks, 17th ed., 2001.

[71] Neyer, A. and Voges, E., "Dynamics of electrooptic bistable devices with delayed feedback," *IEEE J. Quantum Electron.*, vol. 18, pp. 2009–2015, December 1982.

[72] Nielsen, T. and Chandrasekhar, S., "OFC 2004 workshop on optical and electronic mitigation of impairments," *J. Ligthwave Technol.*, vol. 23, pp. 131–142, Jan 2005.

[73] Oppenheim, A. V., Wornell, G. W., Isabelle, S. H., and Cuomo, K. M., "Signal processing in the context of chaotic signals," in *Acoustics, Speech, and Signal Processing, 1992. ICASSP-92., 1992 IEEE International Conference on*, vol. 4, pp. 117–120, March 1992.

[74] Parlitz, U., Chua, L., Kocarev, L., Halle, K., and Shang, A., "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation and Chaos*, vol. 3, no. 4, pp. 973–977, 1992.

[75] Parlitz, U., Lunge, L., and Locarev, L., "Synchronization-based parameter estimation from time series," *Phys. Rev. E.*, vol. 54, pp. 6253–6259, December 1996.

[76] Pauer, M. and Winzer, P. J., "Impact of extinction ratio on RZ gain in optically preamplified receivers," *IEEE Photon. Technol. Lett.*, vol. 15, pp. 879–881, Jun 2003.

[77] Pecora, L. M. and Carroll, T. L., "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, February 1990.

[78] Press, W. H., Flannery, B. P., Teukolsky, S. A., and Vetterling, W. T., *Numerical Recipes in C: The Art of Scientific Computing*. Cambridge University Press, 2nd ed., 1992.

[79] Proakis, J. G., *Digital Communications*. New York: MacGraw Hill, 4th ed., 2001.

[80] Rasmussen, C., Fjelde, T., Bennike, J., Liu, F., Dey, S., der Wagt, P., Akasaka, Y., Harris, D., Gapontsev, D., Ivshin, V., and Reeves-Hall, P., "DWDM 40 G transmission over transpacific distance (10000 km) using CSRZ-DPSK and enhanced FEC and all-Raman amplified 100 km Ultrawave fiber spans," in *Proc. Optical Fiber Communication Conf.(OFC)*, 2001. Paper PD18.

[81] Rivest, R. L., Shamir, A., and Aldeman, L. M., "A method for obtaining digital signatures and public-key cryptosystems," *Communcations of the ACM*, vol. 21, pp. 120–126, February 1978.

[82] Schmid, S., "Lithium niobate to rule 40G modulation," *Ligthwave Europe*, vol. 2, pp. 14–16, November 2003.

[83] Schneier, B., *Applied Cryptography, Second Edition : protocols, algorithms, and source code in C*. John Wiley and Sons, Inc., 1996.

[84] SHF Communication Technologies AG, *Tutorail Note # 5 : Modulation Schemes*, February 2003.

[85] SHF Communication Technologies AG, *Tutorial Note # 3 : Broadband Communication Signals*, February 2003.

[86] Singh, S., *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography*.

[87] Tam, W., Lau, F., Tse, C., and Yip, M., "An approach to calculating the bit-error rate of a coherent chaos-shift keying digital communication system under a noisy multiuser environment," *IEEE Trans. Circuits Syst. I*, vol. 49, pp. 210–223, February 2002.

[88] Tromborg, B. and Mørk, J., "Nonlinear injection locking dynamics and the onset of coherence collapse in external cavity lasers," *IEEE J. Quantum Electron.*, vol. 26, pp. 642–654, April 1990.

[89] Tyndall, J. *Proc. Roy. Inst.*, vol. 1, p. 446, 1854.

[90] Uchida, A., Liu, Y., Fischer, I., Davis, P., and Aida, T., "Chaotic antiphase dynamics and sychronization in multimode semiconductor lasers," *Phys. Rev. A.*, vol. 64, no. 2, p. 023801, 2001.

[91] Udaltsov, V. S., Goedgebuer, J.-P., Larger, L., Cuenot, J.-B., Levy, P., and Rhodes, W. T., "Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations," *Phys. Lett. A*, vol. 308, pp. 54–60, February 2003.

[92] Udaltsov, V. S., Larger, L., Goedgebuer, J.-P., Locquet, A., and Citrin, D. S., "Time delay identification in chaotic cryptosystems ruled by delay-differential equations," *J. Opt. Technol.*, vol. 72, pp. 23–28, May 2005.

[93] Vicente, R., Daudén, J., Colet, P., and Toral, R., "Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delay feedback loop," in *Physics and Simulation of Optoelectronic Devices XI* (Osinski, M., Amano, H., and Blood, P., eds.), vol. 4986 of *Proc. SPIE*, pp. 452–462, 2003.

[94] Vicente, R., Daudén, J., Colet, P., and Toral, R., "Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delayed feedback loop," *IEEE J. Quantum Electron.*, vol. 41, pp. 541–548, April 2005.

[95] Volkovskii, A. and Rulkov, N., "Experimental study of bifurcations at the threshold for stochastic locking," *Sov. Tech. Phys. Lett.*, vol. 15, pp. 249–251, 1989.

[96] Wiener, M. J., "Efficient DES key search," in *CRYPTO '93*, August 1993.

[97] Winzer, P. J., Dorrer, C., Essiambre, R.-J., and Kang, I., "Chirped return-to-zero modulation by imbalanced pulse carver driving signals," *IEEE Photon. Technol. Lett.*, vol. 16, pp. 1379–1381, May 2004.

[98] Winzer, P. J. and Pfennigbauer, M., "Optimum filter bandwidths for optically preamplified RZ and NRZ receivers," *J. Ligthwave Technol.*, vol. 19, pp. 1263–1273, Sept 2001.

[99] Winzer, P. J. and Essiambre, R.-J., "Advanced modulation formats for high-capacity optical transport networks," *J. Ligthwave Technol.*, vol. 24, pp. 4711–4728, December 2006.

[100] Winzer, P. J. and Essiambre, R.-J., "Advanced optical modulation formats," *Proceedings of the IEEE*, vol. 94, pp. 952–985, May 2006.

[101] Winzer, P. and Kalmar, A., "Sensitivity enhancement of optical receivers by impulsive coding," *J. Ligthwave Technol.*, vol. 17, pp. 171–177, Feb 99.

[102] Wooten, E. L., Kissa, K. M., Yi-Yan, A., Murphy, E. J., Lafaw, D. A., Hallemeier, P. F., Maack, D., Attanasio, D. V., Fritz, D. J., McBrien, G. J., and Bossi, D. E., "A review of lithium niobate modulators for fiber-optic communications systems," *IEEE J. Select. Topics Quantum Electron.*, vol. 6, pp. 69–82, January/February 2000.

[103] Zhong, G. and Ayrom, F., "Experimental confirmation of chaos from Chua's circuit," *Int. J. Circuit Theory Appl.*, vol. 13, no. 11, pp. 93–98, 1985.

[104] Zimmermann, P. R., *The Official PGP User's Guide*. MIT Press, 1995.